

EXHIBIT 2

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

J. ALEX HALDERMAN,

Plaintiff,

v.

HERRING NETWORKS, INC., D/B/A
ONE AMERICA NEWS NETWORK,
CHARLES HERRING, ROBERT
HERRING, SR., and CHANEL RION,

Defendants.

Case No. _____

Judge: _____

Mag. Judge: _____

DECLARATION OF J. ALEX HALDERMAN

I, J. ALEX HALDERMAN, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the following is true and correct:

1. My name is J. Alex Halderman. I am the Bredt Family Professor of Computer Science and Engineering, Director of the Center for Computer Security and Society, and Director of the Software Systems Laboratory at the University of Michigan in Ann Arbor, where I have been a faculty member since 2009. My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are

software security, network security, computer forensics, and election cybersecurity. I have published numerous peer-reviewed research papers analyzing security problems in electronic voting systems used in U.S. states and in other countries. I have also investigated methods for improving election security, such as efficient techniques for auditing whether computerized election results match paper ballots. I attach as **Exhibit 2-A** to this Declaration a current copy of my C.V. and its Publications section, which I keep reasonably up-to-date at <https://jhalderm.com>.

2. I serve as co-chair of the State of Michigan's Election Security Advisory Commission, by appointment of the Michigan Secretary of State. I have also performed security testing of electronic voting systems for the Secretary of State of California. I have testified before the U.S. Senate Select Committee on Intelligence and before the U.S. House Appropriations Subcommittee on Financial Service and General Government on the subject of cybersecurity and U.S. elections.

3. I have been retained as an expert witness in multiple lawsuits related to Dominion voting equipment. The Michigan Department of Attorney General engaged me in *Bailey v. Antrim Cnty.*, No. 2020-009238-CZ (Antrim Circuit Court) to investigate errors in Antrim County's November 2020 election night results. Since 2018, I have also served as an expert for a subset of plaintiffs in *Curling v. Raffensperger*, No. 1:17-cv-2989-AT (N.D. Ga.) ("*Curling*"), which challenges the constitutionality of Georgia's election system on security grounds.

4. I am also serving as a testifying expert for Dominion's former Director of Product Strategy and Security Dr. Eric Coomer in defamation lawsuits in Colorado federal and state courts. I was deposed as an expert for Dr. Coomer in *Coomer v. Lindell et al.*, No. 1:22-cv-01129-NYW-SKC (D. Colo.).

5. My prevailing expert compensation rate at the time of this Declaration is \$950/hour.

6. Neither Herring Networks, Inc., d/b/a One America News Network, Charles Herring, Robert Herring, Sr., and Chanel Rion ("OAN") nor any other defendant involved in consolidated discovery proceedings with the case in which OAN seeks to compel me to testify has proposed retaining me as an expert.¹ Nor, in seeking my deposition, has OAN broached a discussion of the payment of my customary expert testimony fees.

7. Although I have expertise concerning election security issues, my knowledge of this issue is hardly unique. For instance, I was one of 59 election security specialists who co-signed a letter in November 2020 calling claims that the presidential election outcome had been hacked "unsubstantiated" and "technically

¹ I understand these other defendants to include Sidney Powell, her law firm and fundraising website, Michael J. Lindell and his company My Pillow, Patrick Byrne, Christina Bobb, and until his recent bankruptcy filings Rudolph Giuliani.

incoherent.”² OAN could retain any of these experts to inform their present litigation.

8. I have on occasion studied and published about voting equipment manufactured or distributed by Dominion Voting Systems using publicly available information. The only such studies using publicly available information that were published prior to November 3, 2020 concern my research approximately 20 years ago into assets then owned by Diebold Election Systems, Inc. which were purchased by Dominion approximately 14 years ago. *See* Ex. 2-A.

9. I have expert opinion and related factual knowledge about the security of Dominion voting equipment that stems directly and exclusively from my expert work in the *Curling* matter. In *Curling*, the Court authorized the plaintiffs to conduct security testing of Georgia’s Dominion voting machines. I carried out this testing subject to a protective order and other strict confidentiality protocols. My findings include the discovery of several vulnerabilities, which I described to the *Curling* court in sealed, live testimony in September 2020 and in an expert report that I submitted with an Attorneys’ Eyes Only designation under seal in *Curling* on July 1, 2021 (my “Expert Report”), a redacted version of which was unsealed by the

² Matt Blaze, J. A. Halderman, Joseph Lorenzo Hall, Harri Hursti, et al., “Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence” (Nov. 16, 2020). Available at <https://www.mattblaze.org/papers/election2020.pdf>. I attach a true and correct copy of this document as **Exhibit 2-B** to this Declaration.

Curling court in June 2023. *See Curling*, ECF Nos. 906 (testimony), 911 (testimony under seal), 1130 (describing Expert Report as Ex. A), 1131 (sealed Expert Report), 1680 (order permitting unsealing of redacted Expert Report), 1681 (publicly filed redacted Expert Report).

10. My Expert Report in *Curling* was not a forensic analysis of the 2020 presidential election. Although the vulnerabilities it describes pose threats to the security of future elections, I have no evidence that any of these vulnerabilities was exploited to affect the outcome of any past election, including the 2020 presidential election.

11. The *Curling* court established and has repeatedly affirmed strict confidentiality requirements regarding the findings in my Expert Report. *See* Protective Order, ECF No. 477 (July 11, 2019); Order, ECF No. 858 (Sept. 2, 2020) (protective order concerning Fulton County, Ga. Dominion equipment provided prior to third hearing on motions for preliminary injunction); Order Amending Order Directing Transfer of Electronic Equipment, ECF No. 1081 (Mar. 26, 2021) (amending ECF No. 858); Order, ECF No. 1249 (Jan. 10, 2022) (denying proposed intervenor Louisiana Secretary of State access to Expert Report); Order, ECF No. 1453 (Aug. 11, 2022) (denying proposed intervenors, including OAN, access to Expert Report); Order, ECF No. 1520 (Oct. 20, 2022) (striking third-party report quoting Expert Report from docket, affirming decision to keep Expert Report under

seal, and contemplating sanctions against non-party Dominion for sharing Expert Report without express authorization). I attach true and correct copies of these *Curling* orders as well as of the order unsealing a redacted version of my Expert Report (ECF No. 1680), as **Exhibit 2-C** to this Declaration.³

12. I have carefully adhered to the *Curling* court's orders regarding the secrecy of my Expert Report and related non-public testimony, and to orders of other courts regarding my non-public testimony and intend and desire to adhere to those orders still in effect in the future. *See* Ex. 2-C, Ex. 2-D.

13. The foregoing is true and correct to the best of my knowledge, information, and belief and is submitted in support of my Motion.

FURTHER DECLARANT SAYETH NOT, this 6th day of September 2024.



J. ALEX HALDERMAN

³I attach true and correct copies of additional protective orders applying to my expert research and testimony in other court cases as **Exhibit 2-D** to this Declaration.

EXHIBIT 2-A



J. Alex Halderman

Bredt Family Professor of Computer Science & Engineering, University of Michigan

Director, University of Michigan Center for Computer Security and Society

Director, Michigan CSE Systems Lab

email: jhalderm@umich.edu [pgp]

office: +1 734-647-1806

Beyster Building, Room 4717
2260 Hayward Street
Ann Arbor, MI 48109-2121

twitter: [@jhalderm](https://twitter.com/jhalderm)

Research and advising

My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Topics that interest me include software security, network security, security measurement, privacy and anonymity, election cybersecurity, censorship resistance, computer forensics, and online crime. I'm also interested in the interaction of technology with law and policy, politics, and international affairs.

Members of my lab include: Braden Crimmins, Erik Chi, and Dhanya Narayanan. Alumni include: Allison McDonald, Matthew Bernhard, Benjamin VanderSloot, David Adrian, Zakir Durumeric, Drew Springall, Eric Wustrow, James Kasten, Max Froehlich, Rose Howell, Steve Sprecher, Travis Finkenauer, Scott Wolchok, Mingye Chen, Nakul Bajaj, Kartikeya Kandula, Gabrielle Beck, Ben Burgess, Carson Hoffman, Ariana Mirian, Deepak Kumar, Josiah Walker, Colleen Swanson, Will Scott.

Teaching

Fall 2024 — EECS 388: Introduction to Computer Security

Fall 2024 — EECS 498.8: Election Cybersecurity

Coursera — Securing Digital Democracy (massive online course)

Selected publications

DVOrder: Ballot Randomization Flaws Threaten Voter Privacy (site)

Braden Crimmins, Dhanya Narayanan, Drew Springall, and J. Alex Halderman
33rd USENIX Security Symposium
Sec '24, Philadelphia, August 2024 — **Best paper award**

The Antrim County 2020 Election Incident: An Independent Forensic Investigation
J. Alex Halderman

31st USENIX Security Symposium
Sec '22, Boston, August 2022 — **Best paper award**

OpenVPN is Open to VPN Fingerprinting

Diwen Xue, Reethika Ramesh, Arham Jain, Michalis Kallitsis, J. Alex Halderman, Jedidiah R. Crandall, and Roya Ensafi
31st USENIX Security Symposium
Sec '22, Boston, August 2022 — **Best paper award — Internet Defense Prize**

Security Analysis of Georgia's ImageCast X Ballot Marking Devices

J. Alex Halderman and Drew Springall

Expert report submitted on behalf of plaintiffs Donna Curling, et al. in *Curling v. Raffensperger*, Civil Action No. 1:17-CV-2989-AT, U.S. District Court for the Northern District of Georgia, July 1, 2021 — blog post; CISA advisory

Can Voters Detect Malicious Manipulation of Ballot Marking Devices?

Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman
41st IEEE Symposium on Security and Privacy
Oakland '20, San Francisco, May 2020 — **Best student paper award**

Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web

Josh Aas, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J. Alex Halderman, Jacob Hoffman-Andrews, James Kasten, Eric Rescorla, Seth Schoen, and Brad Warren
26th ACM Conference on Computer and Communications Security
CCS '19, London, November 2019

DROWN: Breaking TLS using SSLv2 (site)

Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt

25th USENIX Security Symposium

Sec '16, Austin, TX, August 2016 — **Pwnie Award for best crypto attack**

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice (site)

David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann

22nd ACM Conference on Computer and Communications Security
CCS '15, Oct. 2015; reprinted in *Commun. ACM*, 2019 — **Best paper award**

Neither Snow nor Rain nor MITM: An Empirical Analysis of Email Delivery Security
Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein,
Nicholas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, and
J. Alex Halderman

15th ACM Internet Measurement Conference
IMC '15, Tokyo, October 2015 — **Applied Networking Research Prize**

The Matter of Heartbleed (site)

Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman,
Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and
J. Alex Halderman

14th ACM Internet Measurement Conference
IMC '14, Vancouver, November 2014 — **Best paper award**

ZMap: Fast Internet-wide Scanning and its Security Applications (site)

Zakir Durumeric, Eric Wustrow, and J. Alex Halderman

22nd USENIX Security Symposium
Sec '13, Washington, D.C., August 2013

Mining Your Ps and Qs: Widespread Weak Keys in Network Devices (site)

Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman

21st USENIX Security Symposium
Sec '12, Bellevue, WA, August 2012 — **Best paper award — Test of time award**

Telex: Anticensorship in the Network Infrastructure (site)

Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. Alex Halderman

20th USENIX Security Symposium
Sec '11, San Francisco, August 2011 — **PET award runner-up**

Security Analysis of India's Electronic Voting Machines (video)

Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati,
Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp

17th ACM Conference on Computer and Communications Security
CCS '10, Chicago, October 2010

Lest We Remember: Cold Boot Attacks on Encryption Keys (video)

J. Alex Halderman, Seth Schoen, Nadia Heninger, William Clarkson, William Paul,
Joseph A. Calandrino, Ariel Feldman, Jacob Appelbaum, and Edward W. Felten

17th USENIX Security Symposium — **Best student paper award**
Sec '08, San Jose, CA, August 2008; reprinted in *Commun. ACM*, May 2009

Publications

J. Alex Halderman

Peer-reviewed research papers

Ten Years of ZMap

Zakir Durumeric, David Adrian, Phillip Stephens, Eric Wustrow, and J. Alex Halderman
To appear in *24th ACM Internet Measurement Conference (IMC)*, November 2024

DVSorder: Ballot Randomization Flaws Threaten Voter Privacy

Braden L. Crimmins, Dhanya Y. Narayanan, Drew Springall, and J. Alex Halderman
33rd USENIX Security Symposium, August 2024 — **Best Paper Award**

Just add WATER: WebAssembly-based Circumvention Transports

Erik Chi, Gaukas Wang, J. Alex Halderman, Eric Wustrow, Jack Wampler
Workshop on Free and Open Communications on the Internet (FOCI), February 2024

Challenges in Cybersecurity: Lessons from Biological Defense Systems

Edward Schrom, Ann Kinzig, Stephanie Forrest, Andrea L. Graham, Simon A. Levin, Carl T. Bergstrom, Carlos Castillo-Chavez, James P. Collins, Rob J. de Boeri, Adam Doupée, Roya Ensafi, Stuart Feldman, Bryan T. Grenfell, J. Alex Halderman, Silvie Huijben, Carlo Maley, Melanie Mosesr, Alan S. Perelson, Charles Perrings, Joshua Plotkin, Jennifer Rexford, and Mohit Tiwari
Mathematical Biosciences, vol. 362, August 2023

Logic and Accuracy Testing: A Fifty-State Review

Josiah Walker, Nakul Bajaj, Braden L. Crimmins, and J. Alex Halderman
7th International Joint Conference on Electronic Voting (E-Vote-ID '22), October 2022

The Antrim County 2020 Election Incident: An Independent Forensic Investigation

J. Alex Halderman
31st USENIX Security Symposium, August 2022 — **Best Paper Award**

OpenVPN is Open to VPN Fingerprinting

Diwen Xue, Reethika Ramesh, Arham Jain, Michalis Kallitsis, J. Alex Halderman, Jedidiah R. Crandall, and Roya Ensafi
31st USENIX Security Symposium, August 2022 — **Best Paper Award — Internet Defense Prize Winner**

RemoteVote and SAFE Vote: Towards Usable End-to-End Verification for Vote-by-Mail

Braden L. Crimmins, Marshall Rhea, and J. Alex Halderman
7th Workshop on Advances in Secure Electronic Voting, February 2022

Improving the Accuracy of Ballot Scanners Using Supervised Learning

Sameer Barretto, William Chown, David Meyer, Aditya Soni, Atreya Tata, and J. Alex Halderman
6th International Joint Conference on Electronic Voting (E-Vote-ID '21), October 2021

Security Analysis of the Democracy Live Online Voting System

Michael A. Specter and J. Alex Halderman
30th USENIX Security Symposium, August 2021

Investigating Large-Scale HTTPS Interception in Kazakhstan

Ram Sundara Raman, Leonid Evdokimov, Eric Wustrow, J. Alex Halderman, and Roya Ensafi
20th ACM Internet Measurement Conference (IMC), October 2020

Running Refraction Networking for Real

Benjamin VanderSloot, Sergey Frolov, Jack Wampler, Sze Chuen Tan, Irv Simpson, Michalis Kallitsis, J. Alex Halderman, Nikita Borisov, and Eric Wustrow
20th Privacy Enhancing Technologies Symposium (PETS), July 2020

Characterizing Transnational Internet Performance and the Great Bottleneck of China

Pengxiong Zhu, Keyu Man, Zhongjie Wang, Zhiyun Qian, Roya Ensafi, J. Alex Halderman, and Haixin Duan
ACM SIGMETRICS 2020, June 2020

Can Voters Detect Malicious Manipulation of Ballot Marking Devices?

Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman
41st IEEE Symposium on Security and Privacy (Oakland '20), May 2020 —
Best Student Paper Award

Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web

Josh Aas, Richard Barnes, Benton Case, Zakir Durumeric, Peter Eckersley, Alan Flores-López, J. Alex Halderman, Jacob Hoffman-Andrews, James Kasten, Eric Rescorla, Seth Schoen, and Brad Warren
26th ACM Conference on Computer and Communications Security (CCS '19), November 2019

Conjure: Summoning Proxies from Unused Address Space

Sergey Frolov, Jack Wampler, Sze Chuen Tan, J. Alex Halderman, Nikita Borisov, and Eric Wustrow
26th ACM Conference on Computer and Communications Security (CCS '19), November 2019

UnclearBallot: Automated Ballot Image Manipulation

Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman
4th International Joint Conference on Electronic Voting (E-Vote-ID '19), October 2019

On the Usability of HTTPS Deployment

Matthew Bernhard, Jonathan Sharman, Claudia Z. Acemyan, Philip Kortum, Dan S. Wallach, and J. Alex Halderman
ACM Conference on Human Factors in Computing Systems (CHI '19), May 2019

Bernoulli Ballot-Polling: A Manifest Improvement for Risk-Limiting Audits

Kellie Ottoboni, Matthew Bernhard, J. Alex Halderman, Ronald L. Rivest, and Philip B Stark
4th Workshop on Advances in Secure Electronic Voting (Voting '19), February 2019

403 Forbidden: A Global View of Geoblocking

Allison McDonald, Matthew Bernhard, Benjamin VanderSloot, Will Scott, J. Alex Halderman, and Roya Ensafi
18th ACM Internet Measurement Conference (IMC '18), October 2018

Quack: Scalable Remote Measurement of Application-Layer Censorship

Benjamin VanderSloot, Allison McDonald, Will Scott, J. Alex Halderman, and Roya Ensafi
27th USENIX Security Symposium (Sec '18), August 2018

Tracking Certificate Misissuance in the Wild

Deepak Kumar, Zhengping Wang, Matthew Hyder, Joseph Dickinson, Gabrielle Beck, David Adrian, Joshua Mason, Zakir Durumeric, J. Alex Halderman, and Michael Bailey
39th IEEE Symposium on Security and Privacy (Oakland '18), May 2018

Initial Measurements of the Cuban Street Network

Eduardo Pujol, Will Scott, Eric Wustrow, and J. Alex Halderman
17th ACM Internet Measurement Conference (IMC '17), November 2017

Public Evidence from Secret Ballots

Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach
2nd International Joint Conference on Electronic Voting (E-Vote-ID '17), October 2017

Understanding the Mirai Botnet

Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou
26th USENIX Security Symposium (Sec '17), August 2017

An ISP-Scale Deployment of TapDance

Sergey Frolov, Fred Douglas, Will Scott, Allison McDonald, Benjamin VanderSloot, Rod Hynes, Adam Kruger, Michalis Kallitsis, David Robinson, Nikita Borisov, J. Alex Halderman, and Eric Wustrow
7th USENIX Workshop on Free and Open Communications on the Internet (FOCI '17), August 2017

Security Challenges in an Increasingly Tangled Web

Deepak Kumar, Zane Ma, Zakir Durumeric, Ariana Mirian, Joshua Mason, J. Alex Halderman, and Michael Bailey
26th World Wide Web Conference (WWW '17), April 2017

The Security Impact of HTTPS Interception

Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan, Elie Bursztein, Michael Bailey, J. Alex Halderman, and Vern Paxson
24th Network and Distributed Systems Symposium (NDSS '17), February 2017

Measuring Small Subgroup Attacks Against Diffie-Hellman

Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, and Nadia Heninger
24th Network and Distributed Systems Symposium (NDSS '17), February 2017

An Internet-Wide View of ICS Devices

Ariana Mirian, Zane Ma, David Adrian, Matthew Tischer, Thasphon Chuenchujit, Tim Yardley, Robin Berthier, Josh Mason, Zakir Durumeric, J. Alex Halderman, and Michael Bailey
14th IEEE Conference on Privacy, Security, and Trust (PST '16), December 2016

Implementing Attestable Kiosks

Matthew Bernhard, J. Alex Halderman, and Gabe Stocco
14th IEEE Conference on Privacy, Security, and Trust (PST '16), December 2016

A Security Analysis of Police Computer Systems

Benjamin VanderSloot, Stuart Wheaton, and J. Alex Halderman
14th IEEE Conference on Privacy, Security, and Trust (PST '16), December 2016

Measuring the Security Harm of TLS Crypto Shortcuts

Drew Springall, Zakir Durumeric, and J. Alex Halderman
16th ACM Internet Measurement Conference (IMC '16), November 2016

Towards a Complete View of the Certificate Ecosystem

Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. Alex Halderman
16th ACM Internet Measurement Conference (IMC '16), November 2016

Content-Based Security for the Web

Alexander Afanasyev, J. Alex Halderman, Scott Ruoti, Kent Seamons, Yingdi Yu, Daniel Zappala, and Lixia Zhang
2016 New Security Paradigms Workshop (NSPW '16), September 2016

DROWN: Breaking TLS using SSLv2

Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt
25th USENIX Security Symposium (Sec '16), Austin, TX, August 2016 — **Pwnie Award** — **Internet Defense Prize Finalist**

FTP: The Forgotten Cloud

Drew Springall, Zakir Durumeric, and J. Alex Halderman
46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '16), Toulouse, June 2016

Android UI Deception Revisited: Attacks and Defenses

Earlence Fernandes, Qi Alfred Chen, Justin Paupore, Georg Essl, J. Alex Halderman, Z. Morley Mao, and Atul Prakash
20th International Conference on Financial Cryptography and Data Security (FC '16), Barbados, February 2016

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice

David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann
22nd ACM Conference on Computer and Communications Security (CCS '15), Denver, CO, October 2015 — **Best Paper Award** — **Pwnie Award**
Reprinted in *Communications of the ACM*, January 2019

Censys: A Search Engine Backed by Internet-Wide Scanning

Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex Halderman
22nd ACM Conference on Computer and Communications Security (CCS '15), Denver, CO, October 2015

Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security

Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicholas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, and J. Alex Halderman

15th ACM Internet Measurement Conference (IMC '15), Tokyo, Japan, October 2015 — **IRTF Applied Networking Research Prize Winner**

The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election

J. Alex Halderman and Vanessa Teague

5th International Conference on E-voting and Identity (VoteID '15), Bern, Switzerland, September 2015

Umbra: Embedded Web Security through Application-Layer Firewalls

Travis Finkenauer and J. Alex Halderman

1st Workshop on the Security of Cyberphysical Systems (WOS-CPS '15), Vienna, Austria, September 2015

Replication Prohibited: Attacking Restricted Keyways with 3D Printing

Ben Burgess, Eric Wustrow, and J. Alex Halderman

9th USENIX Workshop on Offensive Technologies (WOOT '15), Washington, DC, August 2015

The Matter of Heartbleed

Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. Alex Halderman

14th ACM Internet Measurement Conference (IMC '14), Vancouver, BC, November 2014 — **Best Paper Award**

Security Analysis of the Estonian Internet Voting System

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman

21st ACM Conference on Computer and Communications Security (CCS '14), Scottsdale, AZ, November 2014

Efficiently Auditing Multi-Level Elections

Joshua A. Kroll, Edward W. Felten, and J. Alex Halderman

6th International Conference on Electronic Voting (EVOTE '14), Lochau, Austria, October 2014

Security Analysis of a Full-Body Scanner

Keaton Mowery, Eric Wustrow, Tom Wypych, Corey Singleton, Chris Comfort, Eric Rescorla, Stephen Checkoway, J. Alex Halderman, and Hovav Shacham

23rd USENIX Security Symposium (Sec '14), San Diego, CA, August 2014

TapDance: End-to-Middle Anticensorship without Flow Blocking

Eric Wustrow, Colleen M. Swanson, and J. Alex Halderman

23rd USENIX Security Symposium (Sec '14), San Diego, CA, August 2014

An Internet-Wide View of Internet-Wide Scanning

Zakir Durumeric, Michael Bailey, and J. Alex Halderman

23rd USENIX Security Symposium (Sec '14), San Diego, CA, August 2014

Green Lights Forever: Analyzing the Security of Traffic Infrastructure

William Beyer, Branden Ghena, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman
8th USENIX Workshop on Offensive Technologies (WOOT '14), San Diego, CA, August 2014

Zipper ZMap: Internet-Wide Scanning at 10Gbps

David Adrian, Zakir Durumeric, Gulshan Singh, and J. Alex Halderman
8th USENIX Workshop on Offensive Technologies (WOOT '14), San Diego, CA, August 2014

Elliptic Curve Cryptography in Practice

Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow
18th International Conference on Financial Cryptography and Data Security (FC '14), March 2014

Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security

Alex Migicovsky, Zakir Durumeric, Jeff Ringenberg, and J. Alex Halderman
18th International Conference on Financial Cryptography and Data Security (FC '14), March 2014

Analysis of the HTTPS Certificate Ecosystem

Zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman
13th ACM Internet Measurement Conference (IMC '13), Barcelona, Spain, October 2013

ZMap: Fast Internet-Wide Scanning and its Security Applications

Zakir Durumeric, Eric Wustrow, and J. Alex Halderman
22nd USENIX Security Symposium (Sec '13), Washington, DC, August 2013

Illuminating the Security Issues Surrounding Lights-Out Server Management

Anthony Bonkoski, Russ Bielawski, and J. Alex Halderman
7th USENIX Workshop on Offensive Technologies (WOOT '13), Washington, DC, August 2013

Internet Censorship in Iran: A First Look

Simurgh Aryan, Homa Aryan, and J. Alex Halderman
3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI '13), Washington, DC, August 2013

CAGE: Taming Certificate Authorities by Inferring Restricted Scopes

James Kasten, Eric Wustrow, and J. Alex Halderman
17th International Conference on Financial Cryptography and Data Security (FC '13), Okinawa, Japan, April 2013

Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman
21st USENIX Security Symposium (Sec '12), Bellevue, WA, August 2012 — **Best Paper Award — Test of Time Award (2022)**
Named one of Computing Reviews' Notable Computing Books and Articles of 2012.

Attacking the Washington, D.C. Internet Voting System

Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman
16th Intl. Conference on Financial Cryptography and Data Security (FC '12), Bonaire, February 2012

Telex: Anticensorship in the Network Infrastructure

Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. Alex Halderman

20th USENIX Security Symposium (Sec '11), San Francisco, CA, August 2011 — **Runner-up for 2012 PET Award**

Internet Censorship in China: Where Does the Filtering Occur?

Xueyang Xu, Z. Morley Mao, and J. Alex Halderman

12th Passive and Active Measurement Conference (PAM '11), Atlanta, GA, March 2011

Absolute Pwnage: Security Risks of Remote Administration Tools

Jay Novak, Jonathan Stribley, Kenneth Meagher, and J. Alex Halderman

15th International Financial Cryptography Conference (FC '11), February 2011

Ethical Issues in E-Voting Security Analysis

David G. Robinson and J. Alex Halderman

2nd Workshop on Ethics in Computer Security Research (WECSR '11), March 2011

Security Analysis of India's Electronic Voting Machines

Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp

17th ACM Conference on Computer and Communications Security (CCS '10), Chicago, IL, October 2010

Crawling BitTorrent DHTs for Fun and Profit

Scott Wolchok and J. Alex Halderman

4th USENIX Workshop on Offensive Technologies (WOOT '10), Washington, DC, August 2010

Sketcha: A Captcha Based on Line Drawings of 3D Models

Steven A. Ross, J. Alex Halderman, and Adam Finkelstein

19th International World Wide Web Conference (WWW '10), Raleigh, NC, April 2010

Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs

Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmett Witchel

17th Network and Distributed System Security Symposium (NDSS '10), San Diego, CA, February-March 2010

Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage

Steve Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham

2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop (EVT '09), Montreal, QC, August 2009

Fingerprinting Blank Paper Using Commodity Scanners

William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten

30th IEEE Symposium on Security and Privacy (Oakland '09), Oakland, CA, May 2009

Lest We Remember: Cold Boot Attacks on Encryption Keys

J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten

17th USENIX Security Symposium (Sec '08), San Jose, CA, July 2008 — **Best Student Paper Award — Pwnie Award**

Reprinted in *Communications of the ACM*, May 2009

In Defense of Pseudorandom Sample Selection

Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten

2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08), San Jose, CA, July 2008

You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems

J. Alex Halderman, Eric Rescorla, Hovav Shacham, and David Wagner

2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08), San Jose, CA, July 2008

Harvesting Verifiable Challenges from Oblivious Online Sources

J. Alex Halderman and Brent Waters

14th ACM Conference on Computer and Communications Security (CCS '07), Washington, DC, October 2007

Machine-Assisted Election Auditing

Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten

2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), Boston, MA, August 2007

Security Analysis of the Diebold AccuVote-TS Voting Machine

Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten

2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), Boston, MA, August 2007

Lessons from the Sony CD DRM Episode

J. Alex Halderman and Edward W. Felten

15th USENIX Security Symposium (Sec '06), Vancouver, BC, August 2006

A Convenient Method for Securely Managing Passwords

J. Alex Halderman, Brent Waters, and Edward W. Felten

14th International World Wide Web Conference (WWW '05), Chiba, Japan, May 2005

Privacy Management for Portable Recording Devices

J. Alex Halderman, Brent Waters, and Edward W. Felten

2004 ACM Workshop on Privacy in the Electronic Society (WPES '04), Washington, DC, October 2004

New Client Puzzle Outsourcing Techniques for DoS Protection

Brent Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten

11th ACM Conference on Computer and Communications Security (CCS '04), Washington, DC, October 2004

Early Experiences with a 3D Model Search Engine

Patrick Min, J. Alex Halderman, Michael Kazhdan, and Thomas A. Funkhouser

8th International Conference on 3D Web Technology (Web3D '03), March 2003 — **Best Paper Award**

A Search Engine for 3D Models

Thomas Funkhouser, Patrick Min, Misha Kazhdan, Joyce Chen, J. Alex Halderman, David Dobkin, and David Jacobs

ACM Transactions on Graphics, 22(1):83-105, January 2003

Evaluating New Copy-Prevention Techniques for Audio CDs

J. Alex Halderman

ACM Workshop on Digital Rights Management (DRM '02), Washington, DC, November 2002

Selected other publications

Improving the Security of United States Elections with Robust Optimization

Braden Crimmins, J. Alex Halderman, and Bradley Sturt

Under submission, August 2023

Voter Privacy and VVSG 2.0

Braden Crimmins, Dhanya Narayanan, J. Alex Halderman, and Drew Springall

Public comments in response to U.S. EAC VVSG 2.0 annual review, June 6, 2023

Testimony in Opposition to Internet Voting in Michigan

J. Alex Halderman

Written testimony to the Michigan House Committee on Elections regarding H.B. 4210, May 9, 2023

Remembering Peter Eckersley

J. Alex Halderman

Remarks delivered at his memorial service, March 4, 2023

The DVSorder Vulnerability

Braden Crimmins, Dhanya Narayanan, Josiah Walker, Drew Springall, and J. Alex Halderman

Oct. 2022

ICS Advisory: Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Findings credited to J. Alex Halderman and Drew Springall

CISA/ICS-CERT (ICSA-22-154-01), June 3, 2022

Election Security Problems Still Must Be Addressed

Susan Greenhalgh and J. Alex Halderman

Newsweek, September 27, 2021

Security Analysis of Georgia's ImageCast X Ballot Marking Devices

J. Alex Halderman and Drew Springall

Expert report submitted on behalf of plaintiffs Donna Curling, et al. in *Curling v. Raffensperger*, Civil Action No. 1:17-CV-2989-AT, U.S. District Court for the Northern District of Georgia, Atlanta Division, July 1, 2021

Analysis of the Antrim County, Michigan November 2020 Election Incident

J. Alex Halderman

Expert report prepared for the State of Michigan, March 26, 2021

Elections Should be Grounded in Evidence, Not Blind Trust

Philip B. Stark, Edward Perez, and J. Alex Halderman

Barrons, January 4, 2021

Michigan Election Security Advisory Commission Report and Recommendations

J. Alex Halderman *et al.*
Report prepared for the State of Michigan, October 2020

Internet Voting Is Happening Now—And it could destroy our elections
Rachel Goodman and J. Alex Halderman
Slate, January 15, 2020

Congressional Testimony Regarding Federal Funding for Election Cybersecurity
J. Alex Halderman
Testimony before the U.S. House Appropriations Subcommittee on Financial Service and General Government, Election Security: Ensuring the Integrity of U.S. Election Systems, February 27, 2019

I Hacked an Election. So Can the Russians.
J. Alex Halderman
Video op/ed in collaboration with *The New York Times*, April 5, 2018

Congressional Testimony Regarding Russian Interference in the 2016 U.S. Elections)
J. Alex Halderman
Testimony before the U.S. Senate Select Committee on Intelligence, June 21, 2017

Here's How to Keep Russian Hackers from Attacking the 2018 Elections
J. Alex Halderman and Justin Talbot-Zorn
The Washington Post, June 21, 2017

Practical Attacks on Real-world E-voting
J. Alex Halderman
In Feng Hao and Peter Y. A. Ryan (Eds.), *Real-World Electronic Voting: Design, Analysis and Deployment*, pages 145–171, CRC Press, December 2016

Want to Know if the Election was Hacked? Look at the Ballots
J. Alex Halderman
Posted on Medium, November 23, 2016. (Read by over a million people.)

The Security Challenges of Online Voting Have Not Gone Away
Robert Cunningham, Matthew Bernhard, and J. Alex Halderman
IEEE Spectrum, November 3, 2016

TIVOS: Trusted Visual I/O Paths for Android
Earlence Fernandes, Qi Alfred Chen, Georg Essl, J. Alex Halderman, Z. Morley Mao, and Atul Prakash
University of Michigan Technical Report, May 2014

Tales from the Crypto Community: The NSA Hurt Cybersecurity. Now It Should Come Clean
Nadia Heninger and J. Alex Halderman
Foreign Affairs, October 23, 2013

To Strengthen Security, Change Developers' Incentives
J. Alex Halderman
IEEE Security and Privacy, March/April 2010

Analysis of the Green Dam Censorware System

Scott Wolchok, Randy Yao, and J. Alex Halderman

University of Michigan Technical Report, June 11, 2009

AVC Advantage: Hardware Functional Specifications

J. Alex Halderman and Ariel J. Feldman

Princeton University Computer Science Technical Report TR-816-08, March 8, 2008

Source Code Review of the Diebold Voting System

Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William Zeller

Part of the California Secretary of State's "Top-to-Bottom" Voting Systems Review, July 2007

Digital Rights Management, Spyware, and Security

Edward W. Felten and J. Alex Halderman

IEEE Security and Privacy, January/February 2006

Analysis of the MediaMax CD3 Copy-Prevention System

J. Alex Halderman

Princeton University Computer Science Technical Report TR-679-03, October 2003

EXHIBIT 2-B

Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence

16 November 2020

We are specialists in election security, having studied the security of voting machines, voting systems, and technology used for government elections for decades.

We and other scientists have warned for many years that there are security weaknesses in voting systems and have advocated that election systems be better secured against malicious attack. As the National Academies recently concluded, "There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats." However, notwithstanding these serious concerns, we have never claimed that technical vulnerabilities have actually been exploited to alter the outcome of any US election.

Anyone asserting that a US election was "rigged" is making an *extraordinary* claim, one that must be supported by persuasive and verifiable evidence. Merely citing the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome. It is simply speculation.

The presence of security weaknesses in election infrastructure does not by itself tell us that any election has actually been compromised. Technical, physical, and procedural safeguards complicate the task of maliciously exploiting election systems, as does monitoring of likely adversaries by law enforcement and the intelligence community. Altering an election outcome involves more than simply the existence of a technical vulnerability.

We are aware of alarming assertions being made that the 2020 election was "rigged" by exploiting technical vulnerabilities. However, in every case of which we are aware, these claims either have been unsubstantiated or are technically incoherent. To our collective knowledge, no credible evidence has been put forth that supports a conclusion that the 2020 election outcome in any state has been altered through technical compromise.

That said, it is imperative that the US continue working to bolster the security of elections against sophisticated adversaries. At a minimum, all states should employ election security practices and mechanisms recommended by experts to increase assurance in election outcomes, such as post-election risk-limiting audits.

If you are looking for a good place to start learning the facts about election security, we recommend the recent National Academies of Science, Engineering, and Medicine (NASEM) study, "Securing the Vote", which is available for free download at <https://doi.org/10.17226/25120>.

Signed,

(Affiliations are for identification purposes only; listed alphabetically by surname.)

1. Tony Adams, Independent Security Researcher
2. Andrew W. Appel, Professor of Computer Science, Princeton University
3. Arlene Ash, Professor, University of Massachusetts Medical School
4. Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science; affiliate faculty, Columbia Law, Columbia University
5. Matt Blaze, McDevitt Chair of Computer Science and Law, Georgetown University
6. Duncan Buell, NCR Professor of Computer Science and Engineering, University of South Carolina
7. Michael D. Byrne, Professor of Psychological Sciences and Computer Science, Rice University
8. Jack Cable, Independent Security Researcher
9. Jeremy Clark, NSERC/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies, Concordia Institute for Information Systems Engineering
10. Sandy Clark, Independent Security Researcher
11. Stephen Checkoway, Assistant Professor of Computer Science, Oberlin College
12. Richard DeMillo, Chair, School of Cybersecurity and Privacy and Warren Professor of Computing, Georgia Tech
13. David L. Dill, Donald E. Knuth Professor, Emeritus, in the School of Engineering, Stanford University
14. Zakir Durumeric, Assistant Professor of Computer Science, Stanford University
15. Aleksander Essex, Associate Professor of Software Engineering, Western University, Canada
16. David Evans, Professor of Computer Science, University of Virginia
17. Ariel J. Feldman, Software Engineer
18. Edward W. Felten, Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University
19. Bryan Ford, Professor of Computer and Communication Sciences, Swiss Federal Institute of Technology Lausanne (EPFL)
20. Joshua M. Franklin, Independent Security Researcher
21. Juan E. Gilbert, Banks Family Preeminence Endowed Professor & Chair, University of Florida
22. J. Alex Halderman, Professor of Computer Science and Engineering, University of Michigan
23. Joseph Lorenzo Hall, SVP Strong Internet, Internet Society
24. Harri Hursti, co-founder Nordic Innovation Labs and Election Integrity Foundation
25. Neil Jenkins, Chief Analytic Officer, Cyber Threat Alliance
26. David Jefferson, Lawrence Livermore National Laboratory (retired)
27. Douglas W. Jones, Associate Professor of Computer Science, University of Iowa

28. Joseph Kiniry, Principal Scientist, Galois, CEO and Chief Scientist, Free & Fair
29. Philip Kortum, Associate Professor of Psychological Sciences, Rice University
30. Carl E. Landwehr, Visiting Professor, University of Michigan
31. Maggie MacAlpine, co-founder Nordic Innovation Labs and Election Integrity Foundation
32. Bruce McConnell, former Deputy Under Secretary for Cybersecurity, Department of Homeland Security, (currently) President, EastWest Institute
33. Patrick McDaniel, Weiss Professor of Information and Communications Technology, Penn State University
34. Walter Mebane, Professor of Political Science and of Statistics, University of Michigan
35. Eric Mill, Chrome Security PM, Google
36. David Mussington, Professor of the Practice, School of Public Policy, University of Maryland College Park
37. Peter G. Neumann, Chief Scientist, SRI International Computer Science Lab
38. Lyell Read, Researcher at SSH Lab, Oregon State University
39. Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology
40. Aviel D. Rubin, Professor of Computer Science, Johns Hopkins University
41. Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School
42. Alexander A. Schwarzmann, Dean of Computer and Cyber Sciences, Augusta University
43. Hovav Shacham, Professor of Computer Science, The University of Texas at Austin
44. Micah Sherr, Provost's Distinguished Associate Professor, Georgetown University
45. Barbara Simons, IBM Research (retired)
46. Kevin Skoglund, Chief Technologist, Citizens for Better Elections
47. Michael A. Specter, EECS PhD Candidate, MIT
48. Alex Stamos, Director, Stanford Internet Observatory
49. Philip B. Stark, Professor of Statistics and Associate Dean of Mathematical and Physical Sciences, University of California, Berkeley
50. Jacob Stauffer, Director of Operations, Coherent CYBER
51. Camille Stewart, Cyber Fellow, Harvard Belfer Center
52. Rachel Tobac, Hacker, CEO of SocialProof Security
53. Giovanni Vigna, Professor, Computer Science, University of California, Santa Barbara
54. Poorvi L. Vora, Professor of Computer Science, The George Washington University
55. Dan S. Wallach, Professor, Departments of Computer Science and Electrical & Computer Engineering, Rice Scholar, Baker Institute of Public Policy, Rice University
56. Tarah Wheeler, Cyber Fellow, Harvard Belfer Center
57. Eric Wustrow, Assistant Professor, Department of Electrical, Computer & Energy Engineering, University of Colorado Boulder
58. Ka-Ping Yee, Review Team Member, California Secretary of State's Top-to-Bottom Review of Voting Systems
59. Daniel M. Zimmerman, Principal Researcher, Galois and Principled Computer Scientist, Free & Fair

EXHIBIT 2-C

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

| | | |
|-----------------------------|---|--------------------------|
| DONNA CURLING, et al., |) | |
| |) | |
| Plaintiffs, |) | |
| |) | Civil Action |
| v. |) | |
| |) | File No. 1:17-CV-2989-AT |
| BRAD RAFFENSPERGER, et al., |) | |
| |) | |
| Defendants. |) | |

PROTECTIVE ORDER

The Court enters the following Protective Order (“the Order”), to which the Parties shall be bound, subject to later modification by Court order. It is **HEREBY ORDERED**:

1. Scope and Third Parties. As used in this Order, the term “document” shall mean all documents, electronically stored information, and tangible things within the scope of Fed. R. Civ. P. 26(a)(1)(A)(ii) and 34(a)(1), as well as information derived from such. A draft or non-identical copy is a separate document within the meaning of this term. All documents produced in the course of discovery (“documents”) shall be subject to this Order as set forth below. Any party to this case and all third parties who have received subpoenas (collectively for purposes of this Order, “Designating Parties”) may designate materials as “Confidential” or

“Attorneys’ Eyes Only” under this Order if they make a good faith determination that there is good cause to designate such materials under the terms of this Order and pursuant to Fed. R. Civ. P. 26(c). The Designating Party bears the burden of demonstrating that a designation is appropriate, if challenged.

This Order is subject to the Local Rules of this District and the Federal Rules of Civil Procedure.

2. Confidential Material. Unless such information has previously been deemed a public record under Georgia law by a federal or state court, the following information contained in documents shall be deemed “confidential” for purposes of this Order, subject to challenge by the parties pursuant to procedure provided in Section 11 herein:

a. Particular Voter Information:

- i. The personal telephone numbers of individuals;
- ii. The personal email addresses of individuals or other contact information used for electronic messaging; and,
- iii. Other information that is not public pursuant to federal or Georgia law that could reveal the identity of a specific individual.

b. Particular Information in Agency and Organizational Files:

- i. Non-public information about agency operations that could impede legitimate operations of the agency if publicly disclosed;
 - ii. Non-public information about Plaintiffs' operations that could impede legitimate operations of Plaintiffs' if publicly disclosed; and
 - iii. Information that is not public pursuant to federal or Georgia law that could impede legitimate government interests if publicly disclosed.
- c. Such other information that the parties mutually agree in good faith meets the good cause standard and should be considered "confidential."**
- d. Nothing contained herein prohibits another party or third-party from designating materials as "Confidential" if they make a good faith determination that there is good cause to designate such materials under the terms of this Order and pursuant to Fed. R. Civ. P. 26(c). The Designating Party bears the burden of demonstrating that a designation is appropriate, if challenged.**
- 3. "ATTORNEYS' EYES ONLY" Material: "ATTORNEYS' EYES ONLY" material means information, documents, and things the designating party**

believes in good faith is not generally known to others and which the designating party (i) would not normally reveal to third parties except in confidence or has undertaken with others to maintain in confidence or (ii) believes in good faith is sensitive and protected by a right to privacy under federal or Georgia law or any other applicable privilege or right related to confidentiality or privacy. “ATTORNEYS’ EYES ONLY” material does not include information that has previously been deemed a public record under Georgia law by a federal or state court. The designation is reserved for information that constitutes proprietary or sensitive information that the producing party maintains as confidential in the normal course of its operations such that disclosure could impede legitimate operations, including but not limited to plans and strategy for security, countermeasures and defenses, security audits and investigations, and information regarding software and/or database structure or architecture. “ATTORNEYS’ EYES ONLY” material may include all information, documents, and things referring or relating to the foregoing, including but not limited to copies, summaries, and abstracts of the foregoing, and may be designated as such in the manner described in Section 5. The following information may be deemed “ATTORNEYS’ EYES ONLY” material for the purposes of this order; however, the fact that such information is listed in this order shall not be construed as a waiver of a party’s

objections to the production or disclosure of said information or as an agreement to produce such information absent a further order of this Court:

a. Particular Voter Information:

- i. The social security numbers of individuals, in whole or in part;
- ii. The driver's license numbers of individuals;
- iii. The birth dates of individuals;
- iv. Information that would compromise the secrecy of a voter's ballot if publicly disclosed;
- v. Other government-issued unique identifiers of individuals; and
- vi. Other information that is confidential pursuant to federal or Georgia law that could reveal the identity of a specific individual.

b. Particular Information Regarding Security:

- i. Methods, tools, and instrumentalities of security tests, audits, and investigations, but not findings (unless disclosure of such findings would create an threat to the security of voting systems or other State infrastructure); and
- ii. Information related to security of voting systems that would create an threat to the ongoing security of such systems if publicly disclosed.

4. Designation of “CONFIDENTIAL” Material and Application of Confidentiality Provisions. The designation of material in the form of documents, discovery responses, or other tangible material other than depositions or other pre-trial testimony shall be made by the designating party by affixing the legend “CONFIDENTIAL” on each page containing information to which the designation applies. The designation of deposition testimony shall be in accordance with paragraph 6 below. All material designated “CONFIDENTIAL” that is not reduced to documentary, tangible, or physical form or that cannot be conveniently designated in the manner set forth above shall be designated by the designating party by informing the receiving party of the designation in writing. The confidentiality rules in this Order will apply to all material marked “CONFIDENTIAL.”

a. Basic Principles. A receiving party may use “Confidential” information that is disclosed or produced by any designating party in connection with this case only for prosecuting, defending, or attempting to settle this litigation. “Confidential” material may be disclosed only to the categories of persons and under the conditions described in this Order. “Confidential” material must be stored and maintained by a receiving party at a location and in a secure manner that ensures that access is limited to the persons authorized under this agreement.

b. Disclosure of “Confidential” Information or Items. Unless otherwise ordered by the Court or permitted in writing by the designating party, any material designated “Confidential” may only be disclosed to:

- i. counsel of record in this action, as well as employees and agents of counsel to whom it is reasonably necessary to disclose the information for this litigation;
- ii. experts and consultants to whom disclosure is reasonably necessary for this litigation and who have signed the “Acknowledgment and Agreement to Be Bound” (Exhibit A);
- iii. the Court, court personnel, and court reports and their staff;
- iv. copy or imaging services retained by counsel to assist in the duplication of “Confidential” material;
- v. during, or in preparation for, their depositions, witnesses in the action to whom disclosure is reasonably necessary and who have signed the “Acknowledgement and Agreement to Be Bound” (Exhibit A), unless otherwise agreed by the designating party or ordered by the Court;

- vi. the author or recipient of a document containing the information or a custodian or other person who otherwise possessed or knew the information;
- vii. Parties, only after execution of the “Acknowledgement and Agreement to Be Bound” (Exhibit A); and
- viii. employees, officers, representatives, and directors of Parties, only after execution of the “Acknowledgement and Agreement to Be Bound” (Exhibit A).

c. Filing “Confidential” Material. Before filing “Confidential” material or discussing or referencing such material in court filings, the filing party shall confer with the designating party to determine whether the designating party will remove the “Confidential” designation, whether the document can be redacted, or whether a motion to seal is warranted. If the parties cannot agree on the handling of “Confidential” material in court filings, then the party seeking to file such material must either move to file the material under seal as described in Section III(f)(ii) of this Court’s Standing Order [Doc. 11] or for a court order permitting filing on the public record.

5. Designation of “ATTORNEYS’ EYES ONLY” Material and Application of “ATTORNEYS’ EYES ONLY” Provisions. The designation of

material in the form of documents, discovery responses, or other tangible materials other than depositions or other pre-trial testimony shall be made by the designating party by affixing the legend “ATTORNEYS’ EYES ONLY” on each page containing information to which the designation applies. The designation of deposition testimony shall be in accordance with paragraph 6 below. All material designated “ATTORNEYS’ EYES ONLY” that is not reduced to documentary, tangible, or physical form or that cannot be conveniently designated in the manner set forth above shall be designated by the designating party by informing the receiving party of the designation in writing. All documents designated “ATTORNEYS’ EYES ONLY” by any Party shall be governed by this section.

a. Basic Principles. A receiving party may use “ATTORNEYS’ EYES ONLY” material that is disclosed or produced by another party or by a non-party in connection with this case only for prosecuting, defending, or attempting to settle this litigation. “ATTORNEYS’ EYES ONLY” material may be disclosed only to the categories of persons and under the conditions described in this Order. “ATTORNEYS’ EYES ONLY” material must be stored and maintained by a receiving party at a location and in a secure manner that ensures that access is limited to the persons authorized under this agreement.

b. Disclosure of “ATTORNEYS’ EYES ONLY” Information or Items. Unless otherwise ordered by the Court or permitted in writing by the designating party, any material designated “ATTORNEYS’ EYES ONLY” may only be disclosed to:

- i. counsel of record in this action, as well as employees and agents of counsel to whom it is reasonably necessary to disclose the information for this litigation;
- ii. experts and consultants to whom disclosure is reasonably necessary for this litigation and who have signed the “Acknowledgment and Agreement to Be Bound” (Exhibit A);
- iii. the Court, court personnel, and court reporters and their staff;
- iv. copy or imaging services retained by counsel to assist in the duplication of “ATTORNEYS’ EYES ONLY” material;
- v. during their depositions, witnesses in the action to whom disclosure is reasonably necessary and who have signed the “Acknowledgment and Agreement to Be Bound” (Exhibit A), unless otherwise agreed by the designating party or ordered by the Court;

vi. the author or recipient of a document containing the information or a custodian or other person who otherwise possessed or knew the information;

vii. E-discovery vendors, only after execution of the “Acknowledgement and Agreement to Be Bound” (Exhibit A).

c. **Filing “ATTORNEYS’ EYES ONLY” Material.** Before filing “ATTORNEYS’ EYES ONLY” material or discussing or referencing such material in court filings, the filing party shall confer with the designating party to determine whether the designating party will remove the “ATTORNEYS’ EYES ONLY” designation, whether the document can be redacted, or whether a motion to seal is warranted. If the parties cannot agree on the handling of “ATTORNEYS’ EYES ONLY” material in court filings, then the party seeking to file such material must either move to file the material under seal as described in Section III(f)(ii) of this Court’s Standing Order [Doc. 11] or for a court order permitting filing on the public record.

6. **Designation of Deposition Testimony.** In order to designate deposition testimony as “Confidential” or “ATTORNEYS’ EYES ONLY,” the designating party shall give prompt notice that it will seek the protections of this

Order either at the deposition or within **seven (7) days** after receipt of the deposition transcript, in accordance with the provisions and restrictions of this Order. Unless otherwise designated at or during the deposition, all deposition testimony shall be treated as if designated “Confidential” until the expiration of such seven (7) day period.

7. Documents, Things, and Information Produced by Non-Parties.

Any party may designate as CONFIDENTIAL any documents or things produced by a non-party in this action, including but not limited to documents produced pursuant to an open records requests under O.C.G.A. § 50-18-70 *et seq.*, that contain information deemed CONFIDENTIAL by the designating party by providing written notice of the designation to all counsel of record and to counsel for the disclosing non-party within **seven (7) days** after the designating party receives the produced document or thing. If no party designates the document or thing as CONFIDENTIAL within the seven (7) day period, and if the disclosing non-party has not designated the document or thing as CONFIDENTIAL, then the document or thing shall be considered not to contain any CONFIDENTIAL information.

8. Use of Documents Containing Redacted Confidential Information.

The parties and their counsel and experts agree to redact confidential information from documents before: (a) using such documents at trial, any hearing, or any court

proceeding; (b) attaching such documents to any pleading or filing; or (c) using such documents in any other way where the documents could be seen by the public or by anyone not bound by this Order.

9. Other Redactions. Nothing in this Order precludes the parties from making redactions for privilege or for other legal reasons before documents are produced.

10. Inadvertent Disclosure. A Party that has inadvertently produced “Confidential” Information or “ATTORNEYS’ EYES ONLY” Information without so designating it may at any time re-designate such information as “Confidential” or “ATTORNEYS’ EYES ONLY.” The inadvertent or unintentional disclosure of “Confidential” or “ATTORNEYS’ EYES ONLY” Information shall not be deemed a waiver, in whole or in part, of any Party’s claims of confidentiality. If a Party inadvertently or unintentionally produces “Confidential” Information or “ATTORNEYS’ EYES ONLY” Information without designating it as such in accordance with the provisions of this Order, that Party shall promptly upon discovery, either: (a) demand the return of the “Confidential” or “ATTORNEYS’ EYES ONLY” Information; or (b) furnish a properly marked substitute copy, along with written notice to all Parties that such document or information is deemed “Confidential” or “ATTORNEYS’ EYES ONLY” and should be treated as such in

accordance with the provisions of this Order. Each receiving Party must treat such document or information as “Confidential” or “ATTORNEYS’ EYES ONLY” from the date such notice is received, but each receiving Party shall have no liability for any disclosures of such information that were made prior to re-designation. Disclosure of “Confidential” or “ATTORNEYS’ EYES ONLY” Information prior to the receipt of such notice, if known, shall be reported to the designating Party.

11. Challenge of “Confidential” or “ATTORNEYS’ EYES ONLY” Designations. Any Party who wishes to challenge the propriety of the designation of Information as “Confidential” or “Restricted Confidential” may do so by providing written notice to the Producing Party within **four (4) days** of the designation of the information as “Confidential” or “Restricted Confidential.” The notice shall (a) attach a copy of each document subject to challenge, or identify each such document by production number or other appropriate designation, and (b) set forth the reason for such objection. The objecting Party and the Producing Party shall attempt in good faith to resolve any challenge on an informal basis. If an agreement cannot be reached, the objecting Party may seek a decision from the Court with respect to the propriety of the designation. The subject material will continue to be protected under this Protective Order until the Court orders otherwise. As provided in the Court’s July 2, 2019 Order, (Doc. 446), for any documents produced

by the Counties or municipalities in response to Plaintiffs' Georgia Open Records Act requests that the State intends to retroactively or prospectively designate as "Confidential," Plaintiffs may share the documents with both their experts and the lead Plaintiff-parties in this case if the individual Plaintiffs execute an agreement requiring them to maintain the confidentiality of those documents. Plaintiffs may lodge challenges to the confidentiality designation of any documents and the Court will resolve all timely objections the week of the July 25, 2019 injunction hearing. However, the Court encourages the parties to resolve all such challenges to the greatest extent feasible before that time. Any challenges and requests for the Court to rule on the confidentiality designations for documents the parties anticipate using at the injunction hearing must be filed on the docket **NO LATER THAN JULY 17, 2019.**

12. No Waiver. The inadvertent failure to assert a claim of attorney-client privilege or protection under the work product doctrine shall not constitute a waiver of the right to claim a privilege or protection. Any party may challenge any such claim of privilege or protection on any ground.

13. Order Remains in Effect. This Order shall remain in effect throughout the course of this litigation and during any appeals. Following the termination of this litigation, the Order shall remain in effect for confidential information derived from

properly designated documents, and the Court shall retain jurisdiction to enforce this provision.

14. Destruction of Un-Redacted Documents Containing Confidential Information. This Paragraph applies to documents that contain un-redacted “Confidential” or “Attorneys Eyes Only” information. Within ninety days after final disposition of this case not subject to further appeal, the parties and their counsel and experts, and all other persons having possession, custody, or control of such documents, shall either: (a) return all such documents and any copies thereof to the individual or entity that produced the documents; or (b) destroy hard copies of such documents and all copies thereof with a shredder and make reasonable efforts to delete all electronic copies of such documents from all systems and databases. Notwithstanding the above requirement, the parties are entitled to retain (a) one copy of pleadings containing un-redacted confidential information and (b) un-redacted confidential information that is incorporated in attorney work product so long as the parties restrict access to such information to those persons who are permitted access under the Order.

15. Action by the Court. Nothing in this Order or any action or agreement of a party under this Order limits the Court’s power to make any Orders that may be appropriate with respect to the use and disclosure of any documents produced or

used in discovery or at trial, including the ability to order removal of a “Confidential” or “ATTORNEYS’ EYES ONLY” designation.


16. Order Subject to Modification. This Order shall be subject to modification by the Court on its own motion or on motion of any party or any other person with standing concerning the subject matter. The parties may seek revision of the deadlines for making confidentiality designations and challenges, if necessary, after the conclusion of the preliminary injunction hearing scheduled for July 25 and 26, 2019.

17. No Prior Judicial Determination. This Order is entered based on the presentations and agreements of the parties and for the purpose of facilitating discovery. Nothing herein shall be construed or presented as a judicial determination that any confidential documents or information are subject to protection under Rule 26(c) of the Federal Rules of Civil Procedure or otherwise until such time as the Court may rule on a specific document or issue.

18. Persons Bound. This Order shall take effect when entered and shall be binding upon all counsel and their law firms, the parties and their employees, officers, directors, and agents, testifying and non-testifying experts, and persons made subject to this Order by its terms. This Order shall apply to all “Confidential” or “ATTORNEYS’ EYES ONLY” Information that was produced by any Party after

the submission of this proposed Protective Order to the Court and appropriately marked as such at the time of production.

IT IS SO ORDERED, this 11th day of July, 2019.



AMY TOTENBERG
UNITED STATES DISTRICT JUDGE

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

| | | |
|-----------------------------|---|--------------------------|
| DONNA CURLING, et al., |) | |
| |) | |
| Plaintiff, |) | |
| |) | Civil Action |
| v. |) | |
| |) | File No. 1:17-CV-2989-AT |
| BRAD RAFFENSPERGER, et al., |) | |
| |) | |
| Defendant. |) | |

ACKNOWLEDGMENT AND AGREEMENT TO BE BOUND

The undersigned hereby acknowledges that he/she has read the Protective Order dated July 11, 2019 in the above-captioned action and attached hereto, understands the terms thereof, and agrees to be bound by its terms. The undersigned submits to the jurisdiction of the United States Court for the Northern District of Georgia in matters relating to the Stipulated Protective Order.

The undersigned acknowledges that violation of the Protective Order may result in penalties for contempt of court or any other penalty otherwise imposed by the United States District Court for the Northern District of Georgia.

Signed: _____ by _____ (print name)

Business Address: _____

Date: _____

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

| | | |
|-------------------------------------|---|------------------|
| DONNA CURLING, <i>et al.</i> , | : | |
| | : | |
| | : | |
| Plaintiffs, | : | |
| | : | |
| v. | : | CIVIL ACTION NO. |
| | : | 1:17-CV-2989-AT |
| BRAD RAFFENSPERGER, <i>et al.</i> , | : | |
| | : | |
| | : | |
| Defendants. | : | |

ORDER

This matter is before the Court on Plaintiffs’ Third Joint Request for Production [847], the parties’ Joint Discovery Statement Regarding Urgent Access to Equipment [Doc. 829], and State Defendants’ Objection to the Production of Protected Work Product/Fortalice Report [Doc. 838].

Plaintiffs’ Request for Production No. 9 seeks production of “[a]ny report, studies, findings, audits, evaluations, and/or assessments of actual or potential security breaches or vulnerabilities associated with the Election System since August 1, 2019, including but not limited to new, updated, or supplemental reports prepared by Fortalice Solutions[.]” In response, State Defendants notified Plaintiffs’ counsel in objections that they were withholding from production a November 2019 report prepared by Fortalice Solutions concerning BMDs as protected attorney work product. According to State Defendants, the report was

undertaken for purposes of this litigation at the direction of Ryan Germany, the General Counsel for the Secretary of State, after Plaintiffs filed their operative complaints challenging the BMD system. No other Fortalice Reports were apparently generated or produced in connection with Fortalice's ongoing consulting with the Secretary of State's Office regarding the security and operation of the SOS Office's information and election systems – consulting that had been expressly referenced in the relief section of the Court's Order of August 15, 2019 as well as in the Order itself.¹

Plaintiffs seek to compel production of the Fortalice November 2019 report, requested by the SOS general counsel one month after the Court's order of August 15, 2019, on the assertion that there is “a clear, substantial and compelling need . . . for the only known report by a third-party cybersecurity firm regarding the current election system in Georgia” and there is “no other means for obtaining this information.” (Doc. 838-3.)

In conjunction with their request for the reports, Plaintiffs also now seek access to the BMD voting equipment (and all associated voting equipment, i.e. scanners that count the vote, access cards, etc.) for testing by their experts in advance of the scheduled hearing on the pending motions for preliminary injunction. Plaintiffs did not initially serve a formal discovery request for the equipment, believing they could independently purchase the equipment. After

¹ See, e.g., Order, Doc. 579 at 150 (re remedy), and 75-89 (scope of Fortalice's work and findings in 2017 and 2018 as to data system security vulnerability issues).

they learned no equipment was available for purchase or would be made available for their purchase, Plaintiffs informally sought access to the equipment directly from the Defendants. While the Fulton County Defendants agreed to provide one BMD to the Coalition Plaintiffs for inspection and assessment, the State Defendants declined Plaintiffs' request to provide access or assist Plaintiffs in purchasing the equipment from Dominion, and advised they would not allow Fulton County to loan out its BMD equipment.

Plaintiffs brought these related disputes to the Court's attention on Friday, August 28, 2020. The Court directed the State Defendants to produce the Fortalice report for *in camera* inspection and held discovery conferences with the parties on August 28, 2020 and August 31, 2020.²

The Court has reviewed the November 27, 2019 Report prepared by Fortalice entitled "Voting Process Analysis," the State Defendant's Objection to the Production of the Fortalice Report, and the Curling Plaintiffs' Notice of Authority regarding work product protection.

Based on the information before the Court, it appears that the Fortalice Report falls within the protection afforded by the attorney work product doctrine. Although the Secretary of State has an existing contract with Fortalice for the performance of cybersecurity services and has prepared reports that have been produced as evidence in this case previously, the Court cannot find that the

² The Court recognized the State Defendants' ongoing objections to production of the Fortalice report and production of the BMDs for testing at the August 31, 2020 discovery conference.

analysis of the BMD system undertaken at the direction of counsel in response to Plaintiffs' claims would have been prepared in substantially similar form absent Plaintiffs bringing their challenge to the BMDs in this litigation. *See In re Capital One Consumer Data Security Breach Litigation*, 2020 WL 2731238 at *3-4 (E.D. Va. May 26, 2020) (citing *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007)).³ Accordingly, the Court finds that the Defendants have asserted a valid attorney work product objection to Plaintiffs' request for production of the Fortalice report. However, that does not by itself resolve the discovery dispute.

At the same time that Defendants seek to preclude Plaintiffs' review of Fortalice's technical analysis of the BMD voting system, they also seek to preclude Plaintiffs from performing their own independent analysis of the system. The issues covered by such technical and security analysis fall within the heartland of this lawsuit's serious claims – and thus, Defendants' blocking position on all fronts is not sustainable, in the face of Plaintiffs' demonstration of substantial need in connection with the Fortalice Report's underlying voting data system/security evaluation. For this reason, the Court finds that Plaintiffs have shown a substantial need in turn for an inspection of the BMD voting system components, and in particular at this time, the BMD system and related ballot scanning and associated operational components. Accordingly, the Court **DENIES** Plaintiffs' Request to compel production of the November 2019 Fortalice Report but **GRANTS in part**

³ The Court has reviewed the cases cited by the Curling Plaintiffs to support their argument that the Fortalice Report is not attorney work product. Though relevant, these cases are distinguishable and are not controlling.

Plaintiffs' Joint Request for access to the BMD voting system for purposes of an expert inspection as follows:

1. Per their agreement, the Fulton County Defendants are **DIRECTED** to provide Plaintiffs with one each of the following items needed for testing as described in the Secretary of State's Logic and Accuracy Procedures **NO LATER THAN SEPTEMBER 4, 2020 AT 5:30 P.M.**

- a. Dominion ImageCast X (ICX) Prime 21" BMD;
- b. ImageCast Precint (ICP) Scanner;
- c. 1 box of ballot paper with a minimum of 100 ballots;
- d. Programmed Technician Card;
- e. Programmed Poll Worker Card;
- f. USB Drive containing information from GA ICX BMD programming group;
- g. Print out of Ballot Activation Codes;
- h. Programmed Compact Flash Cards for Polling Place Scanner; and
- i. Programmed Security Key Tab for Polling Place Scanner.

2. Access to and testing of the equipment shall be subject to the terms of the Protective Order entered in this Case on July 11, 2019 at Doc. 477 in order to address the confidentiality and intellectual property concerns raised by the State Defendants and Dominion.

3. Plaintiffs shall arrange for all testing to be video (without sound) recorded continuously by an independent court videographer. This video shall be


made available to Defendants upon the completion of the Plaintiffs' experts' work **NO LATER THAN SEPTEMBER 10, 2020 AT 9:00 A.M.** and shall be supplemented thereafter.⁴

4. The equipment identified in subsection 1 above shall not be put back into service for any election and shall be temporarily sequestered, at a location to be agreed upon, during the pendency of this lawsuit for future testing as necessary in discovery.

5. Plaintiffs shall make financial arrangements with Fulton County to deposit funds to cover the cost of Dominion replacement equipment it will incur.

6. The Court will address issues relating to the Poll Pad equipment in a subsequent Order, as necessary.

IT IS SO ORDERED this 2nd day of September, 2020.



Amy Totenberg
United States District Judge

⁴ The Plaintiffs may also retain a copy of the certified video.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,
Plaintiffs,

v.

BRAD RAFFENSPERGER, ET AL.,
Defendants.

Civil Action No. 1:17-CV-2989-AT

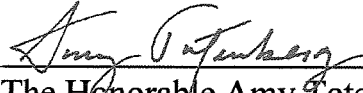
**ORDER AMENDING ORDER DIRECTING TRANSFER OF
ELECTRONIC EQUIPMENT**

This matter is before the Court on Plaintiffs' Consent Motion to Amend Order Directing Transfer of Electronic Equipment [Doc. 1079]. Having considered the Consent Motion, and finding good cause, the Court hereby **GRANTS** the Consent Motion and **AMENDS** its prior Order of September 2, 2020 (Doc. 858) by adding the following paragraph between subsections 3 and 4 of the Order:

3.1. As of March 15, 2021, Plaintiffs shall arrange for all testing to be video (without sound) recorded continuously with a continuous display to include the date, hour, minute, and second of recording by Plaintiffs' counsel or those directly under counsel's supervision at the office of Krevolin & Horst, LLC.

All other terms of the Order shall remain in effect.

SO ORDERED this 26th day of March, 2021.


The Honorable Amy Totenberg
Judge, United States District Court

In his motion, the LA Secretary of State argues that he has a compelling interest in accessing Dr. Halderman’s report because it details multiple potential security flaws in Dominion ICX’s ballot marking device machines, which the State of Louisiana utilizes for early voting. The LA Secretary of State emphasizes that in a subsequent declaration Dr. Halderman “specifically identifie[d] Louisiana as one

of the states at risk from the potential cybersecurity threats.” (Doc. 1243-1 at 3–4.) And he contends that “[a]ccess to Dr. Halderman’s report would enable Louisiana to review his findings, and possibly mitigate some of these potential vulnerabilities in connection with the upcoming 2022 elections.” (*Id.* at 3.)

In a response to the LA Secretary of State’s motion, the State Defendants in this case argue that “Dr. Halderman’s purported reference to the voting machines used for early voting in Louisiana is not a reason to grant Intervener’s motion under Federal Rule of Civil Procedure 24(b).” (Doc. 1244 at 1–2.) Under Rule 24(b), “[o]n timely motion, the court may permit anyone to intervene who: (A) is given a conditional right to intervene by a federal statute; or (B) has a claim or defense that shares with the main action a common question of law or fact.” Accordingly, the State Defendants contend, “Because [the LA Secretary of State] does not have a claim or defense that shares with the main action a common question of law or fact, permissive intervention under Rule 24(b)(1)(B) is not appropriate.” (Doc. 1244 at 2.)

However, as the LA Secretary of State notes, courts have applied a more relaxed approach to Rule 24’s requirements where, as in this case, the movant seeks to intervene for the limited purpose of requesting access to documents subject to a confidentiality order. For example, in *Beckman Industries, Inc. v. International Insurance Co.*, 966 F.2d 470 (9th Cir. 1992), the intervenors sought to intervene in the case for the limited purpose of modifying a protective order. Like the State Defendants here, the defendant in that case argued that the

intervenors had failed to satisfy Rule 24's requirements for permissive intervention because they had failed to identify a claim or defense that was relevant to the action. *Id.* at 473–74. But the court found that “[t]here is no reason to require such a strong nexus of fact or law when a party seeks to intervene only for the purpose of modifying a protective order.” *Id.* at 474. The court opined that “no independent jurisdictional basis” was required because the intervenors were not requesting that the court either rule on additional claims or make them parties to the action. *Id.* at 473. They were simply asking the court to exercise a power that it already had — “the power to modify the protective order.” *Id.*; *see also* 7C Charles Allen Wright et al., *Federal Practice and Procedure* § 1917 (3d ed. 1998) (“A narrow exception to the rule that permissive intervention generally requires an independent jurisdictional basis is when a third party seeks to intervene for the limited purpose of obtaining access to documents protected by a confidentiality order.”).

Similarly, in *E.E.O.C. v. National Children's Center, Inc.*, 146 F.3d 1042 (D.C. Cir. 1998), the court observed that “despite the lack of a clear fit with the literal terms of Rule 24(b)” in these circumstances, “every circuit court that has considered the question has come to the conclusion that nonparties may permissively intervene for the purpose of challenging confidentiality orders.” *Id.* at 1045. Adopting a “flexible approach” toward permissible intervention under Rule 24, and recognizing the “longstanding tradition of public access to court records,” the court construed the Rule as providing “an avenue for third parties to

have their day in court to contest the scope or need for confidentiality.” *Id.* at 1046 (internal quotations marks and citations omitted).

On the other hand, even under this more “flexible approach” to Rule 24, “permissive intervention is an inherently discretionary enterprise,” and courts have discretion to deny motions to permissively intervene even when the requirements of Rule 24 are otherwise satisfied.¹ *Id.* at 1046–48. Notably for purposes of this case, the LA Secretary of State himself acknowledges “the importance of protecting against sensitive voter and cybersecurity information being widely disseminated to the public.” (Doc. 1243-1 at 10.) And as the State Defendants point out, this Court has expressed significant concerns about disseminating the information contained in Dr. Halderman’s report. In spite of these very real concerns, the LA Secretary of State argues that the common law right of public access and the potential injury to voters in the State of Louisiana outweigh any interest in preventing him from accessing Dr. Halderman’s report. While the Court gives great weight to the right of public access to information filed on the docket and the public interest in information regarding elections, it is not persuaded under the specific circumstances presented here that the petitioners’ intervention motion should be granted.

As the LA Secretary of State concedes, the common law right of public access is not absolute; the Court must also consider a number of competing interests that may weigh against disclosure. Those factors include “whether allowing access

¹ The Court takes no position on whether the LA Secretary of State’s motion was timely.

would impair court functions or harm legitimate privacy interests, the degree of and likelihood of injury if made public, the reliability of the information, whether there will be an opportunity to respond to the information, whether the information concerns public officials or public concerns, and the availability of a less onerous alternative to sealing the documents.” (*Id.* at 9–10) (citing *Romero v. Drummond Co., Inc.*, 480 F.3d 1234, 1246 (11th Cir. 2007)). The LA Secretary of State argues that a “less onerous alternative” would be granting him access to Dr. Halderman’s report subject to the Court’s Protective Order. However, the Court remains concerned about the risks associated with further dissemination of the report.² As the Court stated during a prior hearing in which the Coalition Plaintiffs sought to further disseminate the same report, “[a]s it is, I think that we’re on very difficult territory.” (Doc. 1143, Tr. at 66:25–67:1.) The Court still believes this to be true. Further disseminating Dr. Halderman’s report presents complicated risks. Most importantly, sensitive information in the Report relating to the operation of Dominion’s electronic voting software and system could potentially be misused by domestic or foreign hackers or alternatively used for other unlawful or improper purposes. At the current time, if the Court granted the LA Secretary of State access to Dr. Halderman’s report, it could also open the floodgates to similar requests from other individuals and entities around the country, which would also increase the potential for hacking and misuse of

² The Court is not suggesting that the LA Secretary of State would intentionally fail to comply with the Protective Order if he were given access to Dr. Halderman’s report.


sensitive, confidential election system information. Finally, as discussed below, the LA Secretary of State has other reasonable alternatives for assessing the sufficiency of its election system equipment.

For example, the LA Secretary of State could simply reach out to Dr. Halderman himself and request that Dr. Halderman perform a review of the State's election apparatus or Dominion systems on a retained basis. If anything, a targeted investigation of potential cybersecurity threats to Louisiana's own election system would more directly address the LA Secretary of State's concerns than a written report about the system utilized in Georgia. And even if as the LA Secretary of State argues, "the level of analysis and investigation by Dr. Halderman, and other experts, of the Dominion ICX voting system has never occurred previously," (Doc. 1243-1 at 3), that does not mean that a similar analysis and investigation could not be arranged in the future without the LA Secretary of State intervening in this case. In short, the LA Secretary of State has not established that intervening in this case for the purpose of accessing Dr. Halderman's report is an appropriate means of addressing concerns that actually fall within the scope of the LA Secretary of State's authority to investigate the functionality and any vulnerabilities in Louisiana's election system. Such concerns would be more appropriately addressed by retaining Dr. Halderman and other similarly skilled election cyber engineering experts.

The Court has carefully balanced the factors at play in reviewing the LA Secretary of State's intervention request. Given the particular circumstances and

alternatives discussed in this Order as well as consideration of the briefs and factors discussed, the Court **DENIES** the LA Secretary of State's Motion to Intervene [Doc. 1243].

IT IS SO ORDERED this 10th day of January, 2022.


Honorable Amy Totenberg
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

| | | |
|-------------------------------------|---|------------------|
| DONNA CURLING, <i>et al.</i> , | : | |
| | : | |
| Plaintiffs, | : | |
| | : | |
| v. | : | CIVIL ACTION NO. |
| | : | 1:17-cv-2989-AT |
| | : | |
| BRAD RAFFENSPERGER, <i>et al.</i> , | : | |
| | : | |
| Defendants. | : | |

ORDER

Six intervention-related motions are currently before the Court. Four of these motions are Motions to Intervene filed by various companies seeking access to an expert report written by cybersecurity expert Dr. J. Alex Halderman on behalf of the Curling Plaintiffs.¹ The other two motions were filed by one of the proposed intervenors, seeking oral argument on its Motion to Intervene and requesting that the Court lift the stay on the same motion. Dr. Halderman’s report, which concerns potential vulnerabilities in Dominion’s ICX ballot marking device system that is used for elections in the State of Georgia as well as several other States, has been sealed and treated as “Attorneys’ Eyes Only” since it was filed on July 12, 2021 pursuant to the parties’ consent protective order. (Docs. 477, 1130, 1131.) The

¹ Dr. Halderman is a Professor of Computer Science and Engineering at the University of Michigan where he is also director of the Center for Computer Security and Society. He has served as the Curling Plaintiffs’ expert witness on cybersecurity issues since at least 2018.

report was filed in connection with a discovery dispute in this case and has not been filed in connection with a dispositive motion on the merits. (Docs. 1130, 1131.)

I. BACKGROUND

On January 12, 2022, Fox News Network, LLC (“FNN”) filed its Motion to Intervene for the limited purpose of obtaining access to Dr. Halderman’s report on an “Attorneys’ Eyes Only” basis. (Doc. 1251.) The following month, FNN also filed a Motion for Oral Argument on its Motion to Intervene. (Doc. 1303.) On January 27, 2022, Herring Networks, Inc., d/b/a One America News Network (“OAN”), joined FNN’s Motion. (Doc. 1287.) Similarly, on March 2, 2022 and March 5, 2022 respectively, Newsmax, Inc. (“Newsmax”) and My Pillow, Inc. and Michael J. Lindell (collectively, “My Pillow”) moved to intervene in this matter in order to obtain access to Dr. Halderman’s report. (Docs. 1324, 1332.) In addition to seeking access to Dr. Halderman’s report, My Pillow generically seeks access to all documents that have been filed under seal in this matter relating to Dr. Halderman.

FNN, OAN, My Pillow, and Newsmax (collectively, “Proposed Intervenors”) claim in their Motions that they have a compelling need to access Dr. Halderman’s report to aid their respective defenses against defamation claims brought by Dominion in the Delaware Superior Court and the U.S. District Court for the District of Columbia. While Proposed Intervenors contend that Dominion’s defamation claims are based (at least in part) on statements the putative intervenors allegedly made regarding the vulnerability of Dominion’s election

system to hacking or fraud, the claims asserted in Dominion's Complaints appear to focus on very specific purported misrepresentations allegedly made by Proposed Intervenorors that bear little to no relationship to the cyber-security and engineering issues discussed by Dr. Halderman as part of the ongoing litigation in this case. Nevertheless, Proposed Intervenorors argue that Dr. Halderman's report is integral to their defenses in Dominion's lawsuits because it might reveal the truth of their allegedly defamatory statements. For all these reasons, Proposed Intervenorors maintain that it is necessary for them to intervene in the present matter for the purpose of accessing Dr. Halderman's report.

The Court previously stayed all four intervention motions and FNN's Motion for Oral Argument pending the United States Cybersecurity and Infrastructure Agency's ("CISA") review of Dr. Halderman's report and its completion of its formal Coordinated Vulnerability Disclosure ("CVD") process.² (Doc. 1316.) On May 19, 2022, CISA informed the Court that it was undergoing the final steps of its CVD process by continuing to evaluate the potential software vulnerabilities identified in Dr. Halderman's report and beginning to notify relevant government agency stakeholders of specific potential software vulnerabilities in Dominion's election software and the remedies for such. (Doc. 1381.) The next day, although

² Earlier this year, the Court authorized the parties to share an unredacted copy of Dr. Halderman's report with the United States Government's Cybersecurity and Infrastructure Agency ("CISA") on a confidential basis so as to allow CISA to review the report and implement its formal CVD review process.

CISA had not yet completed its CVD process, FNN filed a Motion to Lift the Stay on its Motion to Intervene. (Doc. 1382.)

Several weeks later, CISA completed its CVD process and issued a public advisory detailing its findings. (Doc. 1391); see Cybersecurity & Infrastructure Sec. Agency, ICS Advisory (ICSA-22-154-01): Vulnerabilities Affecting Dominion Voting Systems ImageCast X, (June 3, 2022), <https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01>. The public advisory discusses several potential vulnerabilities affecting Dominion's election software and explains that "[w]hile these vulnerabilities present risks that should be mitigated as soon as possible, CISA has no evidence that these vulnerabilities have been exploited in any elections." *Id.* This CISA advisory information is publicly available to Proposed Intervenors.

Because CISA has completed its review of Dr. Halderman's report and the CVD process, the Court **GRANTS** FNN's Motion to Lift the Stay on its Motion to Intervene (Doc. 1382) and **LIFTS THE STAY** on Proposed Intervenors' Motions to Intervene in this matter. (Docs. 1251, 1287, 1324, and 1332.)

II. DISCUSSION

The Court now turns to the merits of the intervention motions. Proposed Intervenors seek to intervene in this matter pursuant to Federal Rule of Civil Procedure 24. Each putative intervenor argues that it is entitled to intervene in this action as a matter of right or that the Court should exercise its discretion to allow permissive intervention.

A. INTERVENTION AS OF RIGHT

Rule 24(a)(2) allows third parties to intervene as of right in pending litigation where they “claim[] an interest relating to the property or transaction that is the subject of the action[] and [are] so situated that disposing of the action may as a practical matter impair or impede [their] ability to protect [their] interest, unless existing parties adequately represent that interest.” The Eleventh Circuit has explained that a party seeking intervention as of right must demonstrate that:

(1) [their] application to intervene is timely; (2) [they have] an interest relating to the property or transaction which is the subject of the action; (3) [they are] so situated that disposition of the action, as a practical matter, may impede or impair [their] ability to protect that interest; and (4) [their] interest is represented inadequately by the existing parties to the suit.

Burke v. Ocwen Fin. Corp., 833 F. App'x 288 (11th Cir. 2020) (quoting *Tech. Training Assocs., Inc. v. Buccaneers Ltd. P'ship*, 874 F.3d 692, 695–96 (11th Cir. 2017)). Putative intervenors bear the burden of proof to establish all four bases for intervention as a matter of right. *Chiles v. Thornburgh*, 865 F.2d 1197, 1213 (11th Cir. 1989). If putative intervenors fail to establish even one of these elements, intervention as of right must be denied. *Id.*

1. Whether Proposed Intervenors Have an Interest in the Subject of this Action

The Court begins its intervention as of right analysis by considering whether Proposed Intervenors possess an interest relating to the property or transaction that is the subject of this action. “In determining sufficiency of interest, this circuit requires that the intervenor must be at least a real party in interest in the

transaction which is the subject of the proceeding. This interest has also been described as a direct, substantial, legally protectable interest in the proceedings.” *Worlds v. Department of Health and Rehabilitative Serv.*, 929 F.2d 591, 594 (11th Cir.1991) (per curiam) (footnotes, citations, and quotation marks omitted). Thus, a “generalized” concern will not support a claim for intervention as of right. *Athens Lumber Co. v. Fed. Election Comm’n*, 690 F.2d 1364, 1366 (11th Cir. 1982).

Here, Proposed Intervenors have not met their burden to show that they have a direct and substantial interest in the *subject* of this litigation. Each putative intervenor argues that it has an interest in obtaining access to Dr. Halderman’s expert report and the report’s findings relating to potential vulnerabilities in Dominion’s election software. However, the thrust of the Plaintiffs’ claims *in this action* is that the Defendants violated Plaintiffs’ constitutional rights (or those of their members) to cast reliable and verifiable ballots and that, in turn, the Defendants impaired their right to vote. Dr. Halderman’s report is only one document in a sea of documents and testimony filed in this case, and it has not yet been filed in support of or in opposition to a substantive motion on the merits (*i.e.*, a summary judgment motion). None of the Proposed Intervenors have articulated why they have a legally protectible interest in the outcome of this case such that resolving this case without the putative intervenors’ participation would impair their right to protect their interest. Proposed Intervenors are not Georgia voters and could not stand in the shoes of any party in this action. The Court therefore finds that Proposed Intervenors have not met their burden to establish that they

have an interest in the transaction or property that is the subject of this action, which is necessary to entitle them to intervene as of right in this matter.

2. Whether Proposed Intervenorors Are So Situated that Disposition of this Action May Impede or Impair Their Ability to Protect Their Purported Interest

Even if Proposed Intervenorors were able to show that they have a sufficient interest in the subject matter of this proceeding, their claim for intervention as of right would still fail because they have not established that, absent intervention, they will be impaired from protecting their purported interest in obtaining Dr. Halderman's report or the facts described therein. For instance, Proposed Intervenorors could use the discovery channels available in their respective lawsuits as well as retain cybersecurity experts who could provide expert information and opinions directly relevant to the actual claims and defenses asserted in the Dominion lawsuits. Additionally, the putative intervenors could review CISA's public advisory regarding the potential vulnerabilities in Dominion's election software to identify the nature of the election system's vulnerabilities as well as the agency's findings in this connection. *See* Cybersecurity & Infrastructure Sec. Agency, ICS Advisory, *supra*. To the extent that Proposed Intervenorors believe that the available evidence is insufficient to inform their defenses in their respective lawsuits, the judges presiding over those lawsuits are well equipped to determine what additional discovery should be authorized that is tailored to the actual issues at play in the Dominion defamation suits.

Under Rule 26, Proposed Intervenorors are entitled to discovery if it concerns a “nonprivileged matter [and] is relevant to any party’s claim or defense,” *i.e.*, discovery that “appears reasonably calculated to lead to the discovery of admissible evidence.” Fed. R. Civ. P. 26(b)(1).³ Given their familiarity with Dominion’s claims, the judges presiding over the putative intervenors’ respective lawsuits are best suited to determine (1) whether Dr. Halderman’s expert report is relevant to the factual allegations supporting the defamation claims asserted by Dominion in those lawsuits; (2) whether the report is relevant to the putative intervenors’ defenses in those lawsuits; and (3) to what degree Dominion must disclose the report’s contents to Proposed Intervenorors, subject to disclosure limitations imposed by this Court, including this Court’s likely schedule for maintaining full confidentiality of the report through at least the conclusion of the 2022 election cycle.⁴ Therefore, this Court finds that Proposed Intervenorors have not established the likelihood of an impairment of their rights and interests absent their intervention in this matter.

The Court finds it important to note here that, contrary to Proposed Intervenor My Pillow’s assertion in its brief supporting its Motion to Intervene

³ Similarly, under Delaware Superior Court Civil Rule 26(b), Proposed Intervenorors are authorized to serve Dominion a request for documents that are relevant to their defenses. Del. Super. Ct. Civ. R. 26.

⁴ Additionally, the presiding judges will, when compared to the undersigned, be better positioned to weigh the additional factors a court must consider when determining whether to compel production of a particular document in Proposed Intervenorors’ defamation cases, including “the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.” Fed. R. Civ. P. 26(b)(1).

(Doc. 1332-1), the Court never suggested that an earlier proposed intervenor, the Louisiana Secretary of State, hire Dr. Halderman for the purpose of recreating his report in this case. Instead, when the Louisiana Secretary of State moved to intervene in this matter, the Court noted in a January 10, 2022 Order that a “reasonable alternative” to accessing Dr. Halderman’s report would be to:

simply reach out to Dr. Halderman himself and request that Dr. Halderman perform a review of the State’s election apparatus or Dominion systems on a retained basis.

(Doc. 1249 at 6.) The Court then explained that a report based on a targeted investigation of Louisiana’s own election system and the security of that system would likely be more useful than a report describing the potential vulnerabilities in Georgia’s voting system:

If anything, a targeted investigation of potential cybersecurity threats to Louisiana’s own election system would more directly address the LA Secretary of State’s concerns than a written report about the system utilized in Georgia. investigation could not be arranged in the future without the LA Secretary of State intervening in this case.

(*Id.*) Just as the Court did in its January 10th Order, the Court has here considered and described some of the obvious alternatives to intervention in this matter that are specific to the instant parties seeking to intervene and take into account the parties’ objectives and defenses in their own lawsuits.

Because Proposed Intervenors have failed to show that they possess a direct and substantial interest in the subject of this action and that their ability to protect their alleged interests would be impaired if this action were resolved without their

participation, the Court **DECLINES** Proposed Intervenor's requests to intervene in this case as a matter of right.

B. PERMISSIVE INTERVENTION

Having declined Proposed Intervenor's request to intervene as of right in this matter, the Court now considers whether it should exercise its discretion to permit the putative intervenors to intervene in this matter. Under Rule 24(b)(2), "a district court may permit intervention 'when an applicant's claim or defense and the main action have a question of law or fact in common.'" *Athens*, 690 F.2d at 1367 (emphasis added). In determining whether to allow intervention, "the court must consider whether the intervention will unduly delay or prejudice the adjudication of the original parties' rights." Fed. R. Civ. P. 24(b)(3). However, "[i]f there is no right to intervene as of right under Rule 24(a), it is wholly discretionary with the court whether to allow intervention under Rule 24(b) and even though there is a common question of law or fact, or the requirements of Rule 24(b) are otherwise satisfied, the court may refuse to allow intervention." *Burke v. Ocwen Fin. Corp.*, 833 F. App'x 288, 293 (11th Cir. 2020) (quoting *Worlds*, 929 F.2d at 595).

Here, Proposed Intervenor argues that whether Dominion's voting software suffers from security risks or is vulnerable to manipulation are factual questions that play a prominent role both in this matter and Proposed Intervenor's respective cases with Dominion. Relying on *Commissioner, Alabama Department of Corrections v. Advance Loc. Media, LLC*, 918 F.3d 1161, 1173 (11th Cir. 2019), FNN

further argues that the Eleventh Circuit has recognized that putative intervenors who seek to intervene in an action for the limited purpose of accessing a sealed judicial record “provide[] an adequate nexus for intervention under Rule 24(b).” *Id.* at 1173 n.12. The Court reviews these arguments below.

1. Whether There Is a Common Question of Fact Between this Lawsuit and Dominion’s Defamation Lawsuits

First, the Court notes that Dominion’s defamation lawsuits appear to have limited factual overlap with the matter before the Court. In its lawsuit against OAN, Dominion alleges that OAN “manufactured, endorsed, repeated, and broadcast a series of verifiably false yet devastating lies about Dominion.” Compl. ¶ 3, *US Dominion, Inc., et al. v. Herring Networks, Inc., d/b/a One America News Network, et al.*, No. 1:21-cv-02130 (D.D.C. Aug. 10, 2021), ECF No. 1. Dominion’s Complaint continues:

These outlandish and far-fetched fictions included that: (1) Dominion committed election fraud by rigging the 2020 Presidential Election; (2) Dominion’s software and algorithms manipulated vote counts in the 2020 Presidential Election; (3) Dominion is owned by or owns a company founded in Venezuela to rig elections for the dictator Hugo Chávez; and (4) Dominion was involved with alleged voting irregularities in Philadelphia and Dallas—cities where its voting system is not even used.

Id.

In its lawsuit against FNN, Dominion similarly alleges that FNN “endorsed, repeated, and broadcast a series of verifiably false yet devastating lies about Dominion.” Compl. ¶ 2, *U.S. Dominion, Inc., et al., v. Fox News Network, LLC*,

No. N21C-03-257 EMD (Del. Super. Ct. Mar. 26, 2021), ECF No. 1. Dominion's Complaint continues:

These outlandish, defamatory, and far-fetched fictions included Fox falsely claiming that: (1) Dominion committed election fraud by rigging the 2020 Presidential Election; (2) Dominion's software and algorithms manipulated vote counts in the 2020 Presidential Election; (3) Dominion is owned by a company founded in Venezuela to rig elections for the dictator Hugo Chávez; and (4) Dominion paid kickbacks to government officials who used its machines in the 2020 Presidential Election.

Id.

In its lawsuit against Newsmax, Dominion also alleges that Newsmax defamed it by manufacturing, endorsing, repeating, and broadcasting false statements that:

(1) Dominion committed election fraud by rigging the 2020 Presidential Election; (2) Dominion's software and algorithms manipulated vote counts in the 2020 Presidential Election; (3) Dominion is owned by or owns a company founded in Venezuela to rig elections for the dictator Hugo Chávez; (4) Dominion paid kickbacks to government officials who used its machines in swing states during the 2020 Presidential Election; and (5) Dominion was involved with alleged voting irregularities in Dallas, Texas, in 2018—even though Dominion's voting system was not used there.

Compl. ¶ 3, *U.S. Dominion, Inc. v. Newsmax, Inc.*, No. N21C-08-063 EMD (Del. Super. Ct. Aug. 10, 2021), ECF No. 1.

Finally, in its lawsuit against My Pillow, Dominion alleges that My Pillow made or endorsed several false statements that “there were ‘algorithms’ in Dominion machines programmed to steal votes from Trump and that the fraud was discovered in an ‘election night miracle’ when Trump’s lead was so great that

it broke the algorithms.” Compl. ¶ 35, *Dominion v. My Pillow, Inc.*, No. 1:21-cv-00445-CJN (D.D.C. Feb. 22, 2021), ECF No. 1.

Dominion’s defamation lawsuits seemingly contest the veracity of Proposed Intervenor’s statements that Dominion’s “algorithms” manipulated vote counts in the 2020 presidential election by “stealing” votes from former President Donald J. Trump. They also contest the truth of several other statements relating to (1) Dominion’s ownership, (2) alleged kickbacks paid to government officials who used Dominion’s voting software during the 2020 election, and (3) Dominion’s alleged involvement with purported voting irregularities in cities where Dominion’s voting software was not used. Because there appears to be only minimal overlap between the facts and legal issues in this lawsuit and Proposed Intervenor’s asserted defenses in their respective lawsuits, the Court finds that permissive intervention is not warranted here.

2. Whether Proposed Intervenor’s Have a Common Law Right of Access to Dr. Halderman’s Report

Second, the Court addresses the related question of whether Dr. Halderman’s report, even with the redactions proposed by the Plaintiffs,⁵ should be disclosed based on the common law right of public access. The Court recognizes that Proposed Intervenor may be permitted to stand in the shoes of the public and assert a common law right of access to Dr. Halderman’s expert report. *See Nixon v. Warner Commc’ns, Inc.*, 435 U.S. 589, 597 (1978), and *Chicago Trib. Co. v.*

⁵ Previously, the Court directed the Plaintiffs to provide it with proposed redactions to Dr. Halderman’s report.

Bridgestone/Firestone, Inc., 263 F.3d 1304, 1311 (11th Cir. 2001). However, as discussed below, the common law right of public access has yet to attach to Dr. Halderman's report because, at this stage it is merely a record filed in connection with a discovery dispute.

a) The Standard for the Common Law Right of Public Access

"The operations of the courts and the judicial conduct of judges are matters of utmost public concern." *Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829, (1978). Given this, there is a "common-law right of access to judicial proceedings," which includes "the right to inspect and copy public records and documents." *Chicago Trib.*, 263 F.3d at 1311. The right of access is not absolute, however. Instead, "a judge's exercise of discretion in deciding whether to release judicial records should be informed by a 'sensitive appreciation of the circumstances that led to the production of the particular document in question.'" *Id.* at 1311 (cleaned up) (quoting *Nixon*, 435 U.S. at 597). Furthermore, the right of access may be overcome by a showing of good cause, which requires (1) balancing the public's interest in accessing the information against the other party's interest in keeping the information confidential, and (2) considering the "nature and character of the information in question." *See id.* at 1314–15; *Romero v. Drummond Co.*, 480 F.3d 1234, 1246 (11th Cir. 2007).

In performing this balancing act, federal courts consider many case-specific factors, including, but not limited to:

whether allowing access would impair court functions or harm legitimate privacy interests, the degree of and likelihood of injury if made public, the reliability of the information, whether there will be an opportunity to respond to the information, whether the information concerns public officials or public concerns, and the availability of a less onerous alternative to sealing the documents.

Romero, 480 F.3d at 1246.

Importantly, “[w]hen applying the common-law right of access[,] federal courts traditionally distinguish between those items which may properly be considered public or *judicial records* and those that may not.” *F.T.C. v. AbbVie Prod. LLC*, 713 F.3d 54, 62 (11th Cir. 2013) (emphasis added) (citation omitted). The public has a right to access judicial records but do not have a right to access documents that do not qualify as such. *Id.* As “the prospect of all discovery material being presumptively subject to the right of access would likely lead to an increased resistance to discovery requests,” the Eleventh Circuit has recognized a discovery exception to the public right of access. *Romero*, 480 F.3d at 1245. More specifically, the Eleventh Circuit has stated that “material filed with discovery motions is not subject to the common-law right of access, whereas discovery material filed in connection with pretrial motions that require judicial resolution of the merits is subject to the common-law right.” *Chicago Trib.*, 263 F.3d at 1312. That is because the need for the public to access discovery documents is low, as discovery is a private process with trial preparation as its goal. *Romero*, 480 F.3d at 1245. Thus, discovery documents are not judicial documents subject to the common law right of public access.

b) Whether Dr. Halderman's Report Is a Judicial Record Subject to the Common Law Right of Access at this Time

"[W]e determine whether a document is a judicial record depending on the type of filing it accompanied." *AbbVie Prod.*, 713 F.3d at 64. In this case, the Curling Plaintiffs filed Dr. Halderman's expert report on a sealed basis on the docket as a component of a Joint Discovery Statement that did not require "judicial resolution of the merits." (*See* Docs. 1130, 1131.) The Eleventh Circuit has made clear that materials produced in discovery "do not automatically qualify as judicial records subject to the common-law right of access," but only "take on that status once they are filed in connection with a substantive motion." *Callahan v. United Network for Organ Sharing*, 17 F.4th 1356, 1362 (11th Cir. 2021). Because Dr. Halderman's expert report was filed on the docket in connection with a discovery dispute, the common-law right of public access has yet to attach to the report.

Finally, even if Dr. Halderman's expert report were a judicial record or becomes one in the ensuing months, the Court would not likely publicly release the report prior to the full completion of the 2022 election cycle based on the "good cause" standard given associated heightened security issues in the period immediately preceding the election.⁶ If this delay impacts Proposed Intervenors'


⁶ Though this Court has long recognized that "great weight" should be afforded to the public's right to access material filed on the docket, and that there is indeed a strong "public interest in information regarding elections," the Court has also been mindful that "[f]urther disseminating Dr. Halderman's report presents complicated risks" relative to election security. (Doc. 1249 at 4–5.) Releasing Dr. Halderman's report, even with the Plaintiffs' proposed redactions, into the public domain just 89 days before the 2022 General Election could invite hacking and intrusion efforts, especially given the current heated climate surrounding voting issues as well as ever heightening concerns about international and domestic cybersecurity attacks.

discovery and trial schedules, they have an obvious remedy — they can seek an extension of the discovery deadlines in the courts where their cases are being litigated. Accordingly, Proposed Intervenor's request for permissive intervention is **DENIED**.

III. CONCLUSION

For all these reasons, the Court **LIFTS THE STAY** on FNN, OAN, My Pillow, and Newsmax's Motions to Intervene (Docs. 1251, 1287, 1324, and 1332) for the limited purpose of obtaining access to Dr. Halderman's report⁷ and **DENIES** the same Motions. FNN's Motion for Oral Argument (Doc. 1303) is similarly **DENIED as both unnecessary and moot**. To the extent Proposed Intervenor My Pillow also sought to secure from the Court any and all additional sealed documents produced in connection with discovery in this case relating to Dr. Halderman, its Motion is **DENIED** for the reasons discussed above and based on the lack of any meaningful descriptive parameters to this request.

IT IS SO ORDERED this 11th day of August, 2022.


Honorable Amy Totenberg
United States District Judge


⁷ The Court thereby **GRANTS** FNN's Motion to Lift the Stay on its Motion to Intervene (Doc. 1382).

separately filed the full version of the MITRE Report provisionally under seal. (*See* Docs. 1486-1, 1487-1.) Now, in addition to requesting that the full version of the MITRE Report be filed under seal on an official basis, Dominion requests guidance from the Court regarding whether it may share the full version of the MITRE Report with its customers.

As an initial matter, it does not appear that Dominion's Motion is properly before the Court as Dominion is not a party in this case. Furthermore, this Court has repeatedly emphasized that further dissemination of Dr. Halderman's report at this time in the election cycle presents "complicated risks" relative to election security. (*See* Doc. 1453 at 16 n.6) (quoting Doc. 1249 at 4–5). The same is true of the MITRE Report, which directly addresses the very same material contained within Dr. Halderman's report. Moreover, as Plaintiffs previously indicated, Dominion's decision to share Dr. Halderman's report with MITRE NESL in the first place potentially violated the Court's Protective Order. Plaintiffs note that the MITRE Report "quotes extensively from the unredacted Halderman Report—which has been treated as 'Attorneys' Eyes Only' since it issued on July 1, 2021, and has been under seal since filed with the Court on July 12, 2021," and that Dominion has neither sought nor obtained permission to disclose the unredacted version of Dr. Halderman's report to a third party. (Doc. 1506 at 3–4.) By the same token, Dominion's provision of the MITRE Report to its customers at this time would also potentially violate the Court's Protective Order.

Accordingly, Dominion's Motion for Leave to File Under Seal [Doc. 1488] is **DENIED**. The Clerk is **DIRECTED** to remove from the docket the exhibits attached to Dominion's Notice of Filing and Request for Guidance on the Application of the Court's Protective Order (Doc. 1486-1) and Provisionally Sealed Notice of Filing MITRE Report (Doc. 1487-1) on the ground that they were improperly filed.

IT IS SO ORDERED this 20th day of October, 2022.


Honorable Amy Totenberg
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, *et al.*,

Plaintiffs,

V.

BRAD RAFFENSPERGER, *et al.*,

Defendants.

CIVIL ACTION NO.
1:17-cv-2989-AT

ORDER

On January 9, 2023, the State Defendants filed Motions for Summary Judgment against the Curling and Coalition Plaintiffs.¹ (Docs. 1567, 1568.) In support of their Motions for Summary Judgment, the State Defendants filed the “MITRE Report,” which is currently sealed from public view on the docket and described further below. (Doc. 1570-4.) The Plaintiffs oppose the State Defendants’ Motions and rely on the July 2021 report written by cybersecurity expert Dr. J. Alex Halderman (the “Halderman Report”) to support their opposition. (See Docs. 1624, 1636, 1639.) Like the MITRE Report, the Halderman Report is currently sealed from public view on the docket. Indeed, the Halderman Report, which concerns potential vulnerabilities in Dominion’s ICX ballot marking device (“BMD”) system that is used for elections in the State of Georgia as well as several

¹ The Fulton County Defendants similarly filed a Motion for Summary Judgment against the Curling and Coalition Plaintiffs. (Doc. 1571.)

other States, has been sealed and treated as “Attorneys’ Eyes Only” since it was filed on July 12, 2021 pursuant to the parties’ consent protective order. (Docs. 477, 1130, 1131, 1639.) On May 3, 2023, counsel for the Curling Plaintiffs requested via email that the Court unseal the Halderman Report subject to their previously proposed redactions.² It is the Court’s understanding that the State Defendants do not oppose the Curling Plaintiffs’ unsealing request.

In response to a follow-up inquiry from the Court regarding the Curling Plaintiffs’ unsealing request, counsel for the Curling Plaintiffs emailed the Court a series of letters and declarations from various cybersecurity experts in support of their request. These letters and declarations reference not only the Halderman Report but also the MITRE Report — a July 2022 report prepared by the MITRE Corporation’s National Election Security Lab that “undertakes a technical analysis to assess the feasibility of [the Halderman Report]’s proposed attacks [against Georgia’s BMD software] to change the outcome of a Georgia election.” (Doc. 1570-4.) Counsel for the Curling Plaintiffs requested that the letters and declarations be included on the public docket. However, for several reasons, including that the MITRE Report may have been created in violation of this Court’s protective order (see Doc. 1520) and provided to Dominion in contravention of the Court’s prior sealing order, the Curling Plaintiffs contend that the MITRE Report should be struck from the docket. Alternatively, Plaintiffs request that the MITRE Report remain under seal as long as the Halderman Report is under seal and that the

² Importantly, the Curling Plaintiffs previously requested that the Halderman Report be unsealed.

MITRE Report should not be publicly disclosed until Dr. Halderman and the United States Cybersecurity and Infrastructure Agency (the “CISA”) have had the opportunity to review it and propose redactions.

The State Defendants oppose the inclusion of the letters and declarations on the public docket. The State Defendants argue that it would be improper for Plaintiffs to introduce new evidence now that discovery has closed, and that none of these additional materials should be considered for purposes of resolving Defendants’ Motions for Summary Judgment. Alternatively, the State Defendants request that the MITRE Report also be added to the public docket and treated in conjunction with the Halderman Report. The Court addresses each of these issues in turn.

I. The Halderman Report

The Court begins by addressing the Curling Plaintiffs’ request to unseal the redacted version of the Halderman Report. “The operations of the courts and the judicial conduct of judges are matters of utmost public concern.” *Landmark Commc’ns, Inc. v. Virginia*, 435 U.S. 829, 839 (1978). Given this, there is a “common-law right of access to judicial proceedings,” which includes “the right to inspect and copy public records and documents.” *Chicago Trib. Co. v. Bridgestone/Firestone, Inc.*, 263 F.3d 1304, 1311 (11th Cir. 2001). The right of access is not absolute, however. Instead, “a judge’s exercise of discretion in deciding whether to release judicial records should be informed by a ‘sensitive appreciation of the circumstances that led to the production of the particular

document in question.” *Id.* at 1311 (cleaned up) (quoting *Nixon v. Warner Commc’ns, Inc.*, 435 U.S. 589, 597 (1978)). Furthermore, the right of access may be overcome by a showing of good cause, which requires (1) balancing the public’s interest in accessing the information against the other party’s interest in keeping the information confidential, and (2) considering the “nature and character of the information in question.” *See id.* at 1314–15; *Romero v. Drummond Co.*, 480 F.3d 1234, 1246 (11th Cir. 2007).

In performing this balancing act, federal courts consider many case-specific factors, including, but not limited to:

whether allowing access would impair court functions or harm legitimate privacy interests, the degree of and likelihood of injury if made public, the reliability of the information, whether there will be an opportunity to respond to the information, whether the information concerns public officials or public concerns, and the availability of a less onerous alternative to sealing the documents.

Romero, 480 F.3d at 1246.

Importantly, “[w]hen applying the common-law right of access[,] federal courts traditionally distinguish between those items which may properly be considered public or *judicial records* and those that may not.” *F.T.C. v. AbbVie Prod. LLC*, 713 F.3d 54, 62 (11th Cir. 2013) (emphasis added) (citation omitted). The public has a right to access judicial records but does not have a right to access documents that do not qualify as such. *Id.* More specifically, the Eleventh Circuit has stated that “material filed with discovery motions is not subject to the common-law right of access, whereas discovery material filed in connection with

pretrial motions that require judicial resolution of the merits is subject to the common-law right.” *Chicago Trib.*, 263 F.3d at 1312. In other words, materials produced in discovery “do not automatically qualify as judicial records subject to the common-law right of access,” but only “take on that status once they are filed in connection with a substantive motion.” *Callahan v. United Network for Organ Sharing*, 17 F.4th 1356, 1362 (11th Cir. 2021). “[W]e determine whether a document is a judicial record depending on the type of filing it accompanied.” *AbbVie Prod.*, 713 F.3d at 64.

Here, the Curling Plaintiffs originally filed the Halderman Report on the docket as a component of a Joint Discovery Statement that did not require “judicial resolution of the merits.” (See Docs. 1130, 1131.) The Court therefore held in August 2022 (Doc. 1453) that the common-law right of public access had yet to attach to the Report and that it should therefore remain under seal given the serious election security concerns raised by the potential release of the Report even with the Curling Plaintiffs’ proposed redactions.

Since that time, the Halderman Report has been relied on by the Plaintiffs in opposition to the State Defendants’ Motions for Summary Judgment, i.e., substantive motions that require “judicial resolution of the merits.” (See Doc. 1639.) Therefore, the common-law right of public access has now attached to the Report. All parties agree that the Curling Plaintiffs’ proposed redactions to the Halderman Report provide appropriate safeguards against any election security risk and hacking concerns previously raised by the Court. The CISA also agrees

that “Plaintiffs’ most-recent proposed redactions appropriately manage the risk to election security while advancing security through transparency.” (Doc. 1430 at 2.) For all these reasons, the Court **GRANTS** the Curling Plaintiffs’ request to unseal the redacted version of the Halderman Report on the docket for public view.³

Before turning to the MITRE Report, the Court briefly addresses the letters and declarations that the Curling Plaintiffs submitted in support of their request to unseal the Halderman Report. Despite the State Defendants’ objection, the Curling Plaintiffs have recently filed the letters and declarations on the public docket. (Doc. 1678.) These materials were filed on the docket without the Court’s approval. Nevertheless, the Court **GRANTS** the Curling Plaintiffs’ request to file the letters and declarations on the docket *nunc pro tunc*. However, the Court will not consider these materials for purposes of resolving Defendants’ Motions for Summary Judgment.

II. The MITRE Report

Like the Halderman Report, the MITRE Report (Doc. 1570-4) was filed in connection with the State Defendants’ Motions for Summary Judgment, i.e., substantive motions that require “judicial resolution of the merits.” Therefore, the common-law right of public access has now attached to the MITRE Report. Additionally, the Court directed the parties to review and provide any proposed redactions to the MITRE report in order to mitigate and safeguard against any

³ As very small minor corrections have been made in the text of the Halderman report, the Court **DIRECTS** Plaintiffs’ counsel to file the corrected version of the report on the docket and redact only the minimal words that were previously redacted in the sealed version.

potential election security risk associated with the public publication of the MITRE Report. (Doc. 1674.) Counsel for Plaintiffs and Defendants both indicated that no such redactions were necessary. For these reasons, and consistent with this Court's long recognized view that great weight should be afforded to the public's right to access material filed on the docket, the Court **ORDERS** that the MITRE Report be made available for public view. As the Defendants did not seek to make the MITRE Report available to the Plaintiffs during the discovery period prior to summary judgment briefing, the Court will not consider the MITRE report in connection with the summary judgment motion.

III. Conclusion


Having considered the parties' arguments, the Court **GRANTS** the Curling Plaintiffs' request to unseal Dr. Halderman's July 2021 report subject to the Curling Plaintiffs' previously proposed redactions. The Court also **GRANTS** *nunc pro tunc* the Curling Plaintiffs' request to file the additional letters and declarations they provided in support of their request to unseal the Halderman Report. However, the Court will not consider these additional materials for purposes of resolving Defendants' Motions for Summary Judgment.

The Court understands that the Curling Plaintiffs have previously filed the redacted version of the Halderman Report on the docket under seal (Doc. 1639) and that the previously filed version of the Report contains some extremely minor errors. Therefore, the Curling Plaintiffs are **DIRECTED** to file the corrected, redacted version of the Halderman Report on the docket within the next seven

days. The Clerk is **DIRECTED** to permanently seal the previously filed version of the Report that contains errors (Doc. 1639.).

Finally, immediately following the Curling Plaintiffs' filing of the Halderman Report on the docket as ordered (in the next 7 days), the Clerk is **DIRECTED** to unseal the MITRE Report (Doc. 1570-4) so that it will also be available on the public docket in the same time frame.

IT IS SO ORDERED this 7th day of June, 2023.


Honorable Amy Totenberg
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,
Plaintiffs,

v.

BRAD RAFFENSPERGER, ET AL.,
Defendants.

Civil Action No. 1:17-CV-2989-AT

**ORDER AMENDING ORDER DIRECTING TRANSFER OF
ELECTRONIC EQUIPMENT**

This matter is before the Court on Plaintiffs' Consent Motion to Amend Order Directing Transfer of Electronic Equipment [Doc. 1079]. Having considered the Consent Motion, and finding good cause, the Court hereby **GRANTS** the Consent Motion and **AMENDS** its prior Order of September 2, 2020 (Doc. 858) by adding the following paragraph between subsections 3 and 4 of the Order:

3.1. As of March 15, 2021, Plaintiffs shall arrange for all testing to be video (without sound) recorded continuously with a continuous display to include the date, hour, minute, and second of recording by Plaintiffs' counsel or those directly under counsel's supervision at the office of Krevolin & Horst, LLC.

All other terms of the Order shall remain in effect.

SO ORDERED this 26th day of March, 2021.

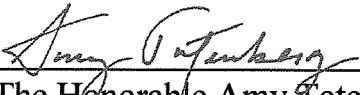

The Honorable Amy Totenberg
Judge, United States District Court

EXHIBIT 2-D

Court finds that entry of a protective order addresses and remedies the objections raised by the Oltmann Defendants. Second, the Court finds that the Oltmann Defendants have not sustained their burden of establishing a basis for their request that Confidential Information be withheld from Plaintiff Coomer.

Accordingly, the Court ORDERS as follows:

This Protective Order shall govern the answers to interrogatories, responses to requests for admission, production of documents, and deposition transcripts, and court filings which contain Confidential Information.

Except as otherwise expressly provided herein or ordered by the Court, Confidential Information as defined above and marked as “Confidential” may be revealed only as follows:

- (a) To counsel for a party (and secretaries, paralegals, and other staff employed in the offices of such counsel who are working on the litigation).
- (b) To the parties and the parties’ directors, officers, employees, or representatives, after such persons have been given a copy of this Protective Order by their counsel and have acknowledged in writing that they agree to be bound by this Protective Order.
- (c) To court reporters transcribing a deposition, hearing, or other proceeding in this matter.
- (d) To independent experts and independent consultants (meaning a person who is not an employee, officer, director, or owner in any capacity of a party and who is retained by a party or a party’s outside counsel in good faith for the purpose of assisting in this litigation) after such persons have been given a copy of this Protective Order by a party’s counsel and have acknowledged in writing that they agree to be bound by this Protective Order.

Confidential Information may be used only for purposes of this litigation. Each person to whom the disclosure of any Confidential Information is made shall not, directly,

or indirectly, use, disclose, or disseminate, or attempt to use, disclose, or disseminate, any of the same except as expressly provided in this Protective Order.

If Confidential Information is to be discussed or disclosed during a deposition or court hearing, a party shall have the right to exclude from attendance at the deposition, during the time the Confidential Information is to be discussed, any person not entitled under this Protective Order to receive the Confidential Information.

Subject to the Colorado Rules of Evidence, Confidential Information may be offered into evidence at trial or at any hearing or oral argument. In the event Confidential Information is used in any pre-trial court filing in this action, the parties are ordered to redact all Confidential Information in a fashion to allow for identification of the witness without disclosing identities (*e.g.*, Person 1, Person 2, etc.).

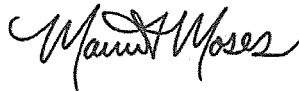
Any motion requesting leave to file unredacted documents containing Confidential Information must be filed in accordance with C.R.C.P. 121, Sec. 1-5.

Nothing in this Order shall constitute an admission by any party that information designated as confidential is Confidential Information. Documents or information available in the public domain, or otherwise previously known by or available to any party, a party's representative(s), directors, officers, and employees, as well as independent experts and consultants hired by counsel, are not rendered confidential solely by disclosure and designation under this stipulation. Furthermore, nothing contained herein shall preclude the parties or a person from raising any available objection or seeking any available protection with respect to any Confidential Information, including

but not limited to the grounds of admissibility of evidence, relevance, trial preparation materials and privilege.

If opposing counsel objects to the designation of certain information as Confidential Information, he or she shall promptly inform the other parties' counsel in writing of the specific grounds of objection to the designation. All counsel shall then, in good faith and on an informal basis, attempt to resolve such dispute. If after such good faith attempt, all counsel are unable to resolve their dispute, opposing counsel may move for a disclosure order consistent with this order. Any motion for disclosure shall be filed within 10 days of receipt by counsel of notice of opposing counsel's objection, and the information shall continue to have Confidential Information status from the time it is produced until the ruling by the Court on the motion.

It is SO ORDERED, this 23rd day of July, 2021.

A handwritten signature in black ink, appearing to read "Marie Avery Moses". The signature is written in a cursive, flowing style.

Honorable Marie Avery Moses
District Court Judge

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Judge Nina Y. Wang**

Civil Action No. 1:22-cv-01129-NYW-SKC

ERIC COOMER, PH.D.,

Plaintiff,

v.

MICHAEL J. LINDELL,
FRANKSPEECH LLC, and
MY PILLOW, INC.,

Defendants.

**PROTECTIVE ORDER GOVERNING THE PRODUCTION AND EXCHANGE OF
CONFIDENTIAL INFORMATION**

Plaintiff Eric Coomer, Ph.D. (“Plaintiff”) and Defendants Michael J. Lindell (“Lindell”), Frankspeech LLC (“Frankspeech”) and My Pillow, Inc. (“MyPillow”) (collectively referred to herein as “Defendants”) are currently engaged in discovery proceedings, which include taking third-party depositions. Discovery proceedings in this action may also include answering interrogatories and producing documents, pending the resolution of Defendants’ Motion for Stay of Discovery [Dkt. 57] and Motion to Dismiss [Dkt. 38].

The Parties believe that certain information that will be produced or that may be produced may contain information that is proprietary, commercially sensitive, subject to a non-disclosure agreement, and/or otherwise non-public. Under Federal Rules of Civil Procedure 5.2 and 26(c), this Order Governing the Production and Exchange of Confidential Information (the “Order”) will govern the handling of documents, testimony (in any form whether by affidavit, declaration, or deposition), exhibits, transcripts, written discovery requests, interrogatory responses, responses to

requests for admission, and responses to requests for documents, and any other information or material produced, given, or exchanged, including any information contained therein or derived therefrom (“Discovery Material”), by or among any Party or non-Party providing Discovery Material, including written and oral responses to discovery requests and/or subpoenas, (each a “Producing Party”) in the above-captioned action (the “Litigation”) to the party receiving the Discovery Material (“Receiving Party”).

1. Any Producing Party may designate any Discovery Material as “Confidential Discovery Material” under the terms of this Order where such Party in good faith believes that such Discovery Material contains trade secrets, proprietary business information, competitively sensitive information or other information the disclosure of which would, in the good faith judgment of the Party or, as appropriate, non-party designating the material as confidential, be detrimental to the conduct of that Party’s or non-party’s business or the business of any of that Party’s or non-party’s customers or clients.

2. Any Producing Party may designate any Discovery Material as “Attorneys’ Eyes Only Discovery Material” under the terms of this Order where such Party in good faith believes that such Discovery Material contains Attorneys’ Eyes Only Discovery Material. Attorneys’ Eyes Only Discovery Material is defined as Confidential Discovery Material containing information such that disclosure other than as provided in this Order could reasonably be expected to cause irreparable harm to the Producing Party. To the extent source code is discoverable, the Parties will meet and confer regarding terms and entry of a separate protective order for the source code before any is permitted to be inspected.

3. The Parties agree that any Confidential Discovery Material and Attorneys’ Eyes Only Discovery Material produced in the Litigation will be used, except by the Producing Party,

solely for purposes of this Litigation and no Receiving Party will provide Discovery Material to any person or entity (including for any other litigation) or make any Discovery Material public except as permitted in this Litigation. Notwithstanding the limitations in the preceding sentence, any Party may use Discovery Material lawfully obtained independently of this Litigation for any purpose consistent with any other limitations placed on that Discovery Material.

4. Notwithstanding any other provision of this Order, no Receiving Party may provide Discovery Material designated as Confidential Material or Attorneys' Eyes Only Material to any person or entity involved in the Litigation unless and until that person or entity confirms their understanding of, and agreement to, abide by the terms of this Order.

5. The designation of Discovery Material as Confidential Discovery Material or Attorneys' Eyes Only Discovery Material will be made in the following manner:

- a. In the case of documents or other written materials (including affidavits and declarations but not pre-trial deposition or other pre-trial testimony: (i) by affixing the legend "Confidential" or "Attorneys' Eyes Only" to each page containing any Confidential or Attorneys' Eyes Only Discovery Material; or (ii) in the case of electronically stored information produced in native format by affixing the legend "Confidential" or "Attorneys' Eyes Only" to the media containing the Discovery Material (e.g., CD, DVD, thumb drive, external hard drive, or secure file transfer).
- b. In the case of testimony: (i) by a statement on the record, by counsel, at the time of such disclosure or, in the case of a deposition or other pre-trial oral testimony, before the conclusion of the deposition or pre-trial testimony; or

(ii) by written notice, sent to all Parties within 15 business days of receipt of the final deposition transcript or other pre-trial testimony; provided that only those portions of the transcript designated as Confidential or Attorneys' Eyes Only Discovery Material will be deemed Confidential or Attorneys' Eyes Only Discovery Material. Each deposition will be deemed to be Attorneys' Eyes Only Discovery Material until 15 business days after counsel receive a copy of the final transcript, after which the deposition will be treated in accordance with its confidentiality designation, if any. The Parties may modify this procedure for any particular deposition, through agreement in writing before, or on the record at, such deposition, without further order of the Court.

- c. In the case of any other Discovery Material, by written notice that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material.

6. The designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material will constitute a representation that such Discovery Material has been reviewed by an attorney of record representing the Party making the designation and that there is a good faith basis for such designation.

7. Inadvertent failure to designate Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material does not constitute a waiver of such claim and may be corrected. A Producing Party may designate as Confidential or Attorneys' Eyes Only any Discovery Material that has already been produced, including Discovery Material that the Producing Party

inadvertently failed to designate as Confidential or Attorneys' Eyes Only, (i) by notifying in writing the Receiving Party to whom the production has been made that the Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material, and (ii) providing a replacement copy of the Discovery Material marked in a manner consistent with Paragraph 5. After receiving such notice, the Parties will treat the Discovery Material so designated as Confidential or Attorneys' Eyes Only Discovery Material, and such Discovery Material will be fully subject to this Order from the date of such supplemental notice forward. The Party receiving such notice will make a reasonable, good -faith effort to ensure that any analyses, memoranda, notes, or other such materials generated that include or are based upon such newly designated information are immediately treated as Confidential or Attorneys' Eyes Only Discovery Material. In addition, after receiving such notice, any receiving Party that disclosed the Discovery Material before its designation as "Confidential" or "Attorneys' Eyes Only" will exercise its best efforts to ensure (i) the return or destruction of such Discovery Material, if it was disclosed to anyone not authorized to receive it under this Order, (ii) that any documents or other materials derived from such Discovery Material are treated as if the Discovery Material had been designated as "Confidential" or "Attorneys' Eyes Only" when originally produced, (iii) that such Discovery Material is not further disclosed except in accordance with the terms of this Order, and (iv) that any such Discovery Material, and any information derived therefrom, is used solely in accordance with this Order.

8. Confidential Discovery Material may be disclosed, summarized, described, characterized, or otherwise communicated, orally or in writing, or made available in whole or in

part only to the following persons for use in connection with the Litigation and in accordance with this Order:

- a. The Parties' current employees who are assisting with or making decisions concerning this Litigation, to the extent deemed reasonably necessary by counsel of record for the purpose of assisting in the prosecution or defense of the Litigation;
- b. Counsel for the Parties in the Litigation (including in-house counsel), and the partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such counsel (including outside copying and litigation support services) who are assisting with the Litigation;
- c. Experts, consultants, or independent litigation support services assisting counsel for the Parties, and partners, associates, paralegals, secretaries, clerical, regular and temporary employees, and service vendors of such experts or consultants (including outside copying services and outside support services) who are assisting with the Litigation;
- d. Persons who appear as an author or recipient on the face of the document to be disclosed;
- e. Witnesses or deponents, and their counsel, but only to the extent necessary to conduct or prepare for depositions or testimony in the Litigation, and only if furnished, shown, or disclosed in accordance with this Order;

- f. The Court, persons employed by the Court, translators, videographers, and court reporters who are recording and transcribing any hearing, trial, or deposition in the Litigation or any appeal therefrom;
- g. A videographer, translator, court reporter, or transcriber who reports, tapes, translates, or transcribes testimony in this Litigation at a deposition and agrees by a statement on the record, before recording or transcribing any such testimony constituting Confidential Discovery Materials, that all such testimony and information revealed at the deposition is and will remain confidential and will not be disclosed by such translator, videographer, reporter, or transcriber except to the attorneys for each Party and any other person who is present while such testimony is being given, and that copies of any transcript, reporter's notes or any other transcription records of any such testimony will be retained in confidentiality and safekeeping by such videographer, translator, reporter, or transcriber or will be delivered to the undersigned attorneys;
- h. Jury consultants and mock jurors, if any, provided each such person executes the form attached as Exhibit A; or
- i. Any other person only upon (i) order of the Court entered upon notice to the Parties, or (ii) written stipulation or statement on the record of agreement by the Producing Party who provided the Discovery Material being disclosed, provided that such person signs an undertaking in the form attached as Exhibit A hereto;

9. Except with the prior written consent of the Producing Party or by Order of the Court, Attorneys' Eyes Only Discovery Material shall not be furnished, shown, or disclosed to any person or entity except to those identified in Paragraph 8(b)–8(i).

10. Confidential or Attorneys' Eyes Only Discovery Material may be provided to persons listed in Paragraph 8(c) only to the extent necessary for such expert or consultant to prepare a written opinion, to prepare to testify, or to assist counsel in the Litigation, provided that such expert or consultant (i) is not subject to a non-disclosure agreement, (ii) agrees to use, and does use, the Discovery Material solely in connection with the Litigation and (iii) agrees to be bound by the terms of this Order by signing an undertaking in the form attached as Exhibit A hereto. Counsel for the Party showing, providing, or disclosing Confidential or Attorneys' Eyes Only Discovery Material to any person required to execute an undertaking under this Paragraph will be responsible for obtaining such signed undertaking and retaining the original, executed copy thereof. "Competitors" are persons or entities endeavoring to engage in the same or similar lines of business, who provide the same or similar services, who sell the same or similar products, or who operate in the same markets, as well as any persons who are engaged in any of these activities.

11. Should the need arise for any Party or non-party to disclose Confidential or Attorney's Eyes Only Discovery Material during any hearing or trial before the Court, including through argument or the presentation of evidence, such Party or non-party may do so only after taking such steps as the Court, upon motion of the Producing Party, deems necessary to preserve the confidentiality of such Confidential or Attorneys' Eyes Only Discovery Material.

12. This Order shall not preclude counsel for any Party from using during any deposition in this action any Documents or Testimony which has been designated as Confidential or Attorneys' Eyes Only Discovery Material under the terms hereof. Any deposition witness who is given access to Confidential or Attorney's Eyes Only Discovery Material shall, prior thereto, be provided with a copy of this Order and shall execute a written agreement, in the form of Exhibit A attached hereto, to comply with and be bound by its terms. Counsel for the Party obtaining the certificate shall supply a copy to counsel for the other Parties and, as appropriate, a non-party that is a Producing Party. If, after being presented with a copy of this Order, a witness refuses to be bound by this Order, the Court shall, upon application, enter an order directing the witness's compliance with the Order.

13. Every person to whom Confidential or Attorneys' Eyes Only Discovery Material is disclosed, summarized, described, characterized, or otherwise communicated or made available, orally or in writing, in whole or in part, will be advised that the information is being disclosed subject to the terms of this Order and may not be disclosed or used for purposes other than those permitted hereunder. Each such person will maintain the Confidential or Attorneys' Eyes Only Discovery Material, or information derived therefrom, in a manner reasonably calculated to prevent unauthorized disclosure. Any Party issuing a subpoena to a non-Party will enclose a copy of this Order and notify the non-Party that the protections of this Order will apply to Discovery Materials of such non-Party.

14. Any pleading, brief, memorandum, motion, letter, affidavit, declaration, or other document filed with the Court that discloses, summarizes, describes, characterizes, or otherwise communicates Confidential or Attorneys' Eyes Only Discovery Materials (a "Confidential Filing") must be filed with the Court under seal in accordance with the Court's Local Rules and Electronic Case Filing Procedures. Nothing in this Order may be construed as restricting any information and/or documents from the public record. To the extent that any Party or non-party seeks to restrict any filing or portion of such filing from public access, it will comply with the requirements of

D.C.COLO.LCivR 7.2.

15. If a Party objects to the designation of Discovery Material as Confidential or Attorneys' Eyes Only Discovery Material, that Party ("the Objecting Party") will send written notice to the Designating Party that includes a date and time for a meet and confer to discuss the disputed designation. The Objecting Party and the Designating Party will thereafter meet and confer either at the suggested date and time or, to the extent the Designating Party is unavailable at the suggested date and time, at some other agreed date and time. If the meet and confer procedure does not resolve the dispute, the Objecting Party may, within seven (7) days of the meet and confer, file a motion with the Court to strike the designation. The Producing Party may, within fourteen (14) days, file a response, and the Objecting Party may file a reply within seven (7) days, after which the matter will be fully briefed and ripe for the Court to resolve the dispute. A hearing may be held at the discretion of the Court. While such an application is pending, the Discovery Material or testimony in question will be treated as Confidential or Attorneys' Eyes Only Discovery Material pursuant to this Order. The burden of establishing that any Discovery Material was properly designated as Confidential or Attorneys' Eyes Only Discovery Material is on the Designating Party. If an Objecting Party seeking to challenge any designation of Discovery Material or testimony as Confidential or Attorneys' Eyes Only fails to object and propose a meet and confer as described in this paragraph, then the Objecting Party will be deemed to have permanently waived its right to challenge the designation of the disputed Discovery Material as Confidential or Attorneys' Eyes Only.

16. The Parties reserve the right to apply under Federal Rules of Civil Procedure 5.2(e) and 26 for an order seeking additional safeguards with respect to the use and handling of Discovery Material or to modify the terms of this Order.

17. Entering into this Order, or agreeing to or producing or receiving Discovery Material or otherwise complying with the terms of this Order, will not:

- a. prejudice in any way the rights of any Party to (i) seek production of any documents or information in discovery, or (ii) object to the production of any documents or information on the ground that it is not subject to discovery;
- b. operate as an admission by any Party that any particular Discovery Material constitutes Confidential or Attorneys' Eyes Only Discovery Material or contains or reflects trade secrets or any other type of confidential information;
- c. prejudice in any way the rights of any Party to (i) petition the Court for a further protective order relating to any purportedly Confidential or Attorneys' Eyes Only Discovery Material, or (ii) seek a determination by the Court whether any Discovery Material or Confidential or Attorneys' Eyes Only Discovery Material should be subject to the terms of this Order;
- d. prevent any Producing Party from agreeing in writing to alter or waive the provisions or protections provided herein with respect to their designation of any particular Discovery Material;
- e. prejudice in any way the rights of any Party to object to the relevance, authenticity, use, or admissibility into evidence of any document, testimony, or other evidence subject to this Order;

- f. preclude any Party from objecting to discovery that it believes to be otherwise improper; or
- g. operate as a waiver of any attorney-client, work product, business strategy, trade secret or other privilege.

18. This Order has no effect upon, and will not apply to, a Producing Party's use or disclosure of its own Discovery Material for any purpose. Nothing herein will prevent a Producing Party from disclosing its own Discovery Material.

19. If Discovery Material that is subject to a claim of attorney-client privilege, attorney work product, or any other applicable privilege or ground on which production of that information should not be made to any Party ("Inadvertent Production Material") is inadvertently produced by a Producing Party or Parties, such inadvertent production, standing alone, will ~~in no way~~ not prejudice or otherwise constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, work product, or other applicable privilege.

- a. A claim of inadvertent production will constitute a representation by the Party claiming inadvertent production that the Inadvertent Production Material has been reviewed by an attorney for the Party claiming inadvertent production and that there is a good faith basis for the claim of inadvertent production.
- b. If a claim of inadvertent production is made under this Order, with respect to Discovery Material then in the custody of another Party, the Party possessing the Inadvertent Production Material will: (i) refrain from any further examination or disclosure of the claimed Inadvertent Production

Material; and (ii) if requested, promptly make a good faith effort to destroy all such claimed Inadvertent Production Material (including summaries and excerpts) and all copies thereof, and certify in writing to that fact. Once a claim of inadvertent production is made, no Party may use the Inadvertent Production Material for any purpose until further order of the Court.

- c. The Party claiming inadvertent production and a Receiving Party will follow the same procedure set forth in this order for challenging the designation of Inadvertent Production Material; while any motion relating to the Inadvertent Production Material is pending, the Inadvertent Production Material in question will be treated in accordance with Paragraph 7. A Receiving Party may not assert as a ground for challenging privilege the fact of the inadvertent production, nor may it include or otherwise disclose in any filing relating to the challenge, as an attachment, exhibit, or otherwise, the Inadvertent Production Material (or any portion thereof).

20. Nothing herein will be deemed to waive any applicable common law or statutory privilege or work product protection.

21. In the event additional Parties join or are joined in the Litigation, they will not have access to Confidential or Attorneys' Eyes Only Discovery Material until the newly joined Party by its counsel has executed this Order and filed with the Court its agreement to be fully bound by it.

22. Subject to the requirements of Federal Rules of Civil Procedure 5.2(e) and 26, the provisions of this Order will, absent written permission of the Designating Party or further order of the Court, continue to be binding throughout and after the conclusion of the Litigation, including, without limitation, any appeals therefrom, except as provided in Paragraph 24.

23. In the event that any Confidential or Attorneys' Eyes Only Discovery Material is used in open court during any court proceeding or filed, marked, or offered as a trial exhibit, the material will lose its confidential status and become part of the public record, unless the Designating Party applies for and obtains an order from this Court specifically maintaining the confidential status of particular material. Before any court proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is to be used, counsel will confer in good faith on such procedures that may be necessary or advisable to protect the confidentiality of any such Discovery Material.

24. Within 60 days after receiving notice of the entry of an order, judgment, or decree finally disposing of the Litigation, or any other proceeding in which Confidential or Attorneys' Eyes Only Discovery Material is permitted to be used, including the exhaustion of all possible appeals, and upon the written request of the Designating or Producing Party, all persons having received Confidential or Attorneys' Eyes Only Discovery Material will either (i) make a good faith and reasonable effort to return such material and all copies thereof (including summaries, excerpts, and derivative works) to counsel for the Producing Party; or (ii) make a good-faith and reasonable effort to destroy all such Confidential or Attorneys' Eyes Only Discovery Material, and certify to that fact in writing to counsel for the Designating or Producing Party. However, counsel for the Parties will be entitled to retain court papers, trial transcripts, and attorney work product containing

Confidential or Attorneys' Eyes Only Discovery Material, provided that such counsel, and employees of such counsel, will maintain the confidentiality thereof and will not disclose such court papers, trial transcripts, or attorney work product containing Confidential or Attorneys' Eyes Only Discovery Material to any person except under a court order or agreement by the Designating and Producing Party or except as otherwise required by law. All materials returned to the Parties or their counsel by the Court likewise will be disposed of in accordance with this paragraph.

25. If any person in possession of Confidential or Attorneys' Eyes Only Discovery Material receives a subpoena or other compulsory process seeking the production or other disclosure of Confidential or Attorneys' Eyes Only Discovery Material the person neither produced nor designated (collectively, a "Demand"), the person will give written notice to counsel for the Designating and Producing Parties within three business days of receipt of such Demand (or if a response to the Demand is due in less than three business days, at least 24 hours prior to the deadline for a response to the Demand), identifying the Confidential or Attorneys' Eyes Only Discovery Material sought and enclosing a copy of the Demand, and must object to the production of the Confidential or Attorneys' Eyes Only Discovery Material on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand will fall on the Designating Party. Nothing herein will be construed as requiring the person receiving the Demand or anyone else covered by this Order to challenge or appeal any order requiring production of Confidential or Attorneys' Eyes Only Discovery Material covered by this Order, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from this Court or any other court. Compliance by the person receiving the Demand with any court order directing

production under a Demand of any Confidential or Attorneys' Eyes Only Discovery Material will not constitute a violation of this Order.

26. Absent a court order, no person who is not a party to the Litigation who receives Confidential or Attorneys' Eyes Only Discovery Material as permitted under the terms of this Order ("a Non-Party") will reveal any Confidential or Attorneys' Eyes Only Discovery Material or the information contained therein, to anyone not entitled to receive such Confidential or Attorneys' Eyes Only Discovery Material under the terms of this Order. In the event that Confidential or Attorneys' Eyes Only Discovery Material is disclosed to any person other than in the manner authorized by this Order, or that any information comes to the non-party's attention that may indicate there was or is likely to be a loss of confidentiality of any Confidential or Attorneys' Eyes Only Discovery Material, the non-party responsible for the disclosure or loss of confidentiality will immediately inform the Designating and Producing Party of all pertinent facts relating to the disclosure or loss of confidentiality, including, if known, the name, address, and employer of each person to whom the disclosure was made. The non-party responsible for the disclosure or loss of confidentiality will also make reasonable efforts to prevent disclosure of Confidential or Attorneys' Eyes Only Discovery Material by each unauthorized person who receives the information.

27. The Parties agree that the production of any Discovery Material by any non-party is subject to and governed by the terms of this Order. The Parties will provide a copy of this Protective Order to all non-parties from whom they seek discovery.

28. If a Party or non-party subject to the jurisdiction of this Court violates this Order by intentionally releasing or otherwise disclosing Confidential or Attorneys' Eyes Only Discovery Material to persons or entities not entitled to such material under this Order or learns of the disclosure of such material and does not immediately

inform the Designating and Producing Party, the Court may impose sanctions under Federal Rule of Civil Procedure 37(b)(2)(A)(i)-(vi).

29. This Court will retain jurisdiction over all persons subject to this Order to the extent necessary to enforce any obligations arising hereunder or to impose sanctions for any contempt thereof.

SO ORDERED.

DATED: November 16, 2022

BY THE COURT:

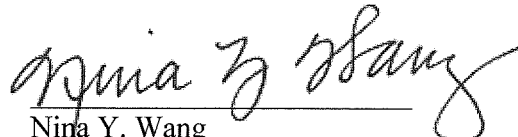

Nina Y. Wang
United States District Judge

EXHIBIT A

Coomer, v. Lindell, et al., Case No. 1:22-cv-01129-NYW-SKC

I have read the Protective Order Dated _____, 2022 in this action (the “Order”) and undertake to access and use Discovery Material, Confidential Material, and Attorneys’ Eyes Only Material only as the Order permits.

Signed this ____ day of _____, 2022.

[Name]

STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY,

Plaintiff,

v

File No. 2020009238CZ
HON. KEVIN A. ELSENHEIMER

ANTRIM COUNTY,

Defendant.

Matthew S. DePerno (P52622)
Attorney for Plaintiff

Haider A. Kazim (P66146)
Attorney for Defendant

DECISION AND ORDER REGARDING
PLAINTIFF'S MOTION FOR AN EX PARTE TEMPORARY RESTRAINING ORDER,
SHOW CAUSE ORDER AND PRELIMINARY INJUNCTION

The above captioned Plaintiff is a resident of Central Lake Township, Antrim County, Michigan. Plaintiff voted in person in the most recent election held November 3, 2020. Subsequently, Plaintiff filed a complaint on November 23, 2020, including the following counts: (1) constitutional right to accuracy and integrity of elections; (2) violation of "purity of elections clause;" (3) election fraud [pursuant to] MCL 600.4545(2) and MCL 158.861; (4) common law election fraud; (5) equal protection violation; and (6) statutory election law violations. Along with his complaint, the Plaintiff also filed a Motion for an Ex Parte Restraining Order, Show Cause Order and Preliminary Injunction. The proposed order, submitted by Plaintiff, would permit Plaintiff to take forensic images from the 22 precinct tabulators and investigate those images, thumb drives, software and the County Clerk's "master tabulator."¹ Additionally, the order would

¹ Defendant asserts that there is no "master tabulator" and that the Dominion tabulator in its possession is the same type used by the individual precincts.

prohibit destruction of evidence relating to the November 3, 2020 election and prohibit turning on the Dominion tabulators or connecting the tabulators to the internet.

The Court heard oral arguments on the Plaintiff's motion on December 3, 2020, and took the matter under advisement. For purposes of this Decision and Order, the Court adopts the Defendant's statement of facts as to the events leading up to and immediately after the election. Moreover, the Defendant has agreed to preserve and protect all records in its possession used to tabulate votes in Antrim County, to not turn on the Dominion tabulator in its possession and to not connect the Dominion tabulator in its possession to the internet.² Therefore, the only remaining issue to be considered by the Court is whether the Plaintiff is permitted to obtain the requested forensic images.

Injunctive relief is generally considered an extraordinary remedy that issues where justice requires, there is an inadequate remedy at law, and there is a real and imminent danger of irreparable injury.³ A preliminary injunction requires a particularized showing of irreparable harm; an injunction will not lie upon the mere apprehension of future injury or where the threatened injury is speculative or conjectural.⁴ To determine whether an injury constitutes irreparable harm, as would support a preliminary injunction the injury is evaluated in light of the totality of the circumstances affecting, and the alternatives available to, the party seeking injunctive relief.⁵ The irreparable-harm factor is considered an indispensable requirement for a preliminary injunction.⁶ In determining whether to issue a preliminary injunction, the trial court must evaluate whether: (1) the moving party made the required demonstration of irreparable harm, (2) the moving party showed that it is likely to prevail on the merits, (3) the harm to the applicant absent such an injunction outweighs the harm it would cause to the adverse party, and (4) there will be harm to the public interest if an injunction is issued.⁷

First, Plaintiff asserts that he will suffer irreparable harm via the loss of his constitutional right to have his vote counted if the temporary restraining order and preliminary injunction are not granted. Specifically, in the recent election, the Village of Central Lake included a proposed

² According to Defendant, it only retains possession of one Dominion tabulator machine. The remaining Dominion tabulator machines are in the custody, control and/or possession of the 22 individual precincts.

³ *Mich AFSCME Council 25 v Woodhaven-Brownstone School Dist*, 293 Mich App 143; 809 NW2d 444 (2011).

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Detroit Fire Fighters Ass'n v City of Detroit*, 482 Mich 18; 753 NW2d 579 (2008).

initiated ordinance to authorize one marihuana retailer establishment within the village on the ballot. There were 524 votes cast regarding this proposal, with 262 for and 262 against. According to the tabulation on November 3, 2020, with the votes tied the proposal failed. However, when the ballots were retabulated on November 6, 2020, the result went from a tied vote to the proposal passing by one vote.⁸ According to the Clerk of Central Lake Township and the ASOG Forensic Report, three ballots were damaged when they were retabulated. Allegedly the damaged ballots were manually re-filled out and re-run through the tabulation machine, yet the final numbers do not reflect that the damaged/cured ballots were included. Plaintiff argues that failure to include the damaged ballots in the retabulation resulted in the marihuana proposal passing and violated his constitutional right to have his vote counted. The temporary, let alone total, loss of a constitutional right constitutes irreparable harm which cannot be adequately remedied by an action at law.⁹ As such, the Court finds that Plaintiff has met the requirement for irreparable harm.

Second, Plaintiff asserts that he is likely to prevail on the merits of his claim because, pursuant to the Michigan Constitution and by statute, his right to vote was violated and he is entitled to have the results of the recent election audited in order to ensure its accuracy and integrity. Defendant counters that Plaintiff is not likely to succeed on the merits of his claims because he lacks standing to bring the constitutional claims and his statutory claims are inapplicable.

A litigant has standing whenever there is a legal cause of action, but even if no legal cause of action is available, a litigant may have standing if he or she has a special injury or right or substantial interest that will be detrimentally affected in a manner different from the citizenry at large or if the statutory scheme implies that the Legislature intended to confer standing on the litigant.¹⁰ While the Defendant argues that Plaintiff has failed to allege an injury in fact, the Court disagrees. As discussed above, assuming that Plaintiff's ballot was one of those damaged during the retabulation, failure to include his vote on the marihuana proposal potentially resulted in passage of the ordinance. Moreover, failure to include the Plaintiff's ballot would amount to the loss of his right to vote, which is an injury specific to Plaintiff. As the Court has determined that

⁸ See Declaration of Judith L. Kosloski.

⁹ *Garner v Mich State Univ*, 185 Mich App 750; 462 NW2d 832 (1990).

¹⁰ *Lansing School Ed. Ass'n v Lansing Bd of Ed.*, 487 Mich 349, 372; 792 NW2d 686 (2010).

the Plaintiff has standing to bring the constitutional claims, it is unnecessary to analyze whether the Plaintiff will succeed on the merits of his statutory claims.¹¹

Third, Plaintiff asserts he will suffer greater harm than the Defendant if the injunction is not granted as he will lose his constitution freedom to vote, whereas the Defendant has a duty to ensure the election process is conducted without fraud. Defendant argues that granting the Plaintiff's request for preliminary injunction would violate the License Agreement with Dominion and essentially force Antrim County to commit breach of contract. The Plaintiff is entitled to have his vote counted and the Defendant has a duty to maintain an accurate and secure election. The Court believes that Defendant's duty to ensure that no eligible Antrim County voter is disenfranchised outweighs its potential duties or obligations under the Licensing Agreement. Moreover, MCR 2.302(C) allows for protective orders that trade secrets or other confidential research, development or commercial information not be disclosed or be disclosed only in a designated way. Thus, any forensic investigation into the Dominion voting equipment can be limited to safeguard the company's intellectual property through a protective order.

Finally, Plaintiff asserts the public interest weighs in favor of granting temporary injunctive relief because confidence in the integrity of our electoral process is essential to the functioning of our participatory democracy. Defendant claims that harm to the public interest, via reverse engineering of Dominion software (presumably for malicious purposes), outweighs any potential harm to the Plaintiff. The Court believes that confirming the accuracy, integrity and security of the electoral process is a greater public interest at this juncture than the potential future misuse of reverse engineered data. Therefore, the public interest weighs in favor of granting the Plaintiff's preliminary injunction.

For the reasons stated herein, the Court finds that Plaintiff has met the necessary requirements for issuance of a preliminary injunction and thus, Plaintiff's Motion for an Ex Parte Restraining Order, Show Cause Order and Preliminary Injunction is granted.

¹¹ MCL § 600.4545(1) applies whenever it appears that material fraud or error has been committed at any election at which there has been submitted any constitutional amendment, question, or proposition to the electors of the state or any county, township or municipality thereof. Defendant argues that this statute is inapplicable because any fraud or error would not have affected the outcome of the election.

IT IS ORDERED that Antrim County maintain, preserve and protect all records in its possession used to tabulate votes in Antrim County, to not turn on the Dominion tabulator in its possession and to not connect the Dominion tabulator in its possession to the internet.

IT IS FURTHER ORDERED, pursuant to MCR 2.302(C), that to protect the respective interests of the parties, this Decision and Order shall also serve as a Protective Order restricting use, distribution or manipulation of the forensic images and/or other information gleaned from the forensic investigation without further order of this Court.

IT IS SO ORDERED.



12/04/2020
05:11PM

KEVIN A. ELSENHEIMER, CIRCUIT COURT JUDGE, P49293

HONORABLE KEVIN A. ELSENHEIMER
Circuit Court Judge

FILED

Sheryl Guy
Antrim 13th Circuit Court
12/15/2020

STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY

Plaintiff

Case No. 20-9238-CZ

v.

ANTRIM COUNTY

HON. KEVIN A. ELSENHEIMER

Defendant.

Matthew S. DePerno (P52622)
DEPERNO LAW OFFICE, PLLC
Attorney for Plaintiff
951 W. Milham Avenue
PO Box 1595
Portage, MI 49081
(269) 321-5064

Haider A. Kazim (P66146)
CUMMINGS, MCCLOREY, DAVIS & ACHO, PLC
Attorney for Defendant
319 West Front Street
Suite 221
Traverse City, MI 49684
(231) 922-1888

Heather S. Meingast (P55439)
Erik A. Grill (P64713)
Assistant Attorneys General
Attorneys for Proposed Intervenor-Defendant
Benson
PO Box 30736
Lansing, MI 48909
(517) 335-7659

**ORDER GRANTING PLAINTIFF'S AMENDED EMERGENCY EX PARTE MOTION
AND BRIEF FOR RELIEF FROM ORDER AND FOR CLARIFICATION OF SCOPE**

At a session of said Court held in the Circuit Court for the County of
Antrim, State of Michigan, on the ____ day of December 2020

PRESENT: HONORABLE KEVIN A. ELSENHEIMER
Circuit Court Judge

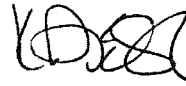
This matter having come before the Court on Plaintiff's Amended Emergency Ex Parte
Motion and Brief for Relief from Order and for Clarification of Scope; the parties having filed
briefs and having appeared through counsel of record on December 14, 2020, at which time the
Court heard oral argument, and the Court being otherwise advised in the premises;.

IT IS HEREBY ORDERED that Plaintiff's motion is **GRANTED** for the reasons stated on the record. Plaintiff and his attorney are permitted to release the Preliminary Antrim Michigan Forensics Report, subject to the redactions discussed on the record and approved by counsel for Defendant Secretary of State. The parties and their attorneys are permitted to use, distribute, or discuss the findings, results, and/or other information gleaned from the forensic investigation as they see fit. The protective order is vacated in all other respects.

IT IS SO ORDERED.

This is not a final order and does not resolve all claims in this Court.

Dated: December ____, 2020



12/15/2020
03:24PM

KEVIN A. ELSENHEIMER, CIRCUIT COURT JUDGE, P49293

Honorable Kevin A. Elsenheimer
Circuit Court Judge

I stipulate and agree to entry of this Order as to form, and waive the seven day notice set forth in MCR 2.602(B)(3):

Dated: December 14, 2020

/s/ Matthew S. DePerno
Matthew S. DePerno (P52622)
Attorney for Plaintiff

Dated: December 14, 2020

/s/ Heather S. Meingast (with permission)
Heather S. Meingast (P55439)
Erik A. Grill (P64713)
Attorneys for Secretary of State

Dated: December 14, 2020

s/ Haider A. Kazim (with permission)
Haider A. Kazim (P66146)
Attorney for Antrim County

From: [Matthew DePerno](#)
To: [Grill, Erik \(AG\)](#)
Cc: [Allan C. Vander Laan](#); [Meingast, Heather \(AG\)](#); [Richards, Margaret \(AG\)](#)
Subject: Re: Bailey v Antrim Co -- Protective Order
Date: Thursday, August 12, 2021 11:21:23 AM
Attachments: [image001.png](#)

CAUTION: This is an External email. Please send suspicious emails to abuse@michigan.gov

Eric,

Understood and just to be clear, on Wednesday at 9:49 am, as soon as I heard, I sent the following cease and desist demand to Mike Lindell.

“This is a demand that you immediately cease and desist disclosing or displaying any forensic images of Antrim County. Those images are under protective order. Neither you or your team are permitted to display or use those images.”

Matt

On Thu, Aug 12, 2021 at 7:44 AM Grill, Erik (AG) <GrillE@michigan.gov> wrote:

We have received information that during an event earlier this week, Mike Lindell publicly displayed or distributed images of the Antrim County EMS software. As a result, we are taking this opportunity to remind all parties of Judge Elsenheimer’s January 11, 2021 order from the bench:

THE COURT: All right. Well, we did discuss
25 this matter to some degree, but I don't think we quite
1 reached the issue of distribution of forensic images,
2 but for those matters that were contained in the
3 expert opinion that was prepared for Mr. Deperno.
4 Those matters are already open. They're
5 available to the public. However, anything that is
6 not included, including individual images in the
7 report, is still subject to in a -- a protective

8 order. And should Mr. Deperno need to provide those
9 images to other experts that he's already identified,
10 then that certainly would be appropriate.
11 However, the Court is not interested in
12 creating unnecessary intrusions into source code,
13 number one, that may be retained, or controlled, or
14 owned by parties that are not part of this litigation,
15 including Dominion. And to the extent that includes
16 forensic imaging -- pardon me, to the extent that
17 includes imaging -- forensic implies some level of
18 analysis, then it makes sense that we -- we also
19 protect that information.
20 So the line I'm trying to draw here,
21 gentlemen, is between matters that are owned as
22 intellectual property by parties that are not part of
23 this litigation, Dominion, et cetera, and those
24 matters that have been released pursuant to my order
25 that have been part of the analysis performed by
1 experts in this case. Again, Mr. Deperno's experts
2 should have the opportunity to review those materials,
3 as should the experts of any other entity -- be it the
4 intervenor, or the county, or any of the other
5 defendants in this case. But mass distribution of
6 that information is not something that the Court is
7 countenancing at this time.

Pages 42-44 of Transcript.

Please ensure that all experts, or individuals working with or for experts, are taking

appropriate action to protect confidential information.

Erik A. Grill

Assistant Attorney General

Civil Litigation, Elections, & Employment Division

517.335.7193

517.335.335.7640 (fax)



--
Sent from Gmail Mobile